Administrator's Guide

Citrix MetaFrame Application Server for Windows

Version 1.8

Citrix Systems, Inc.

Document Code mf.admin.1.8

Contents

Welcome to Citrix MetaFrame

MetaFrame Application Server for Windows is Citrix's server-based computing solution for Microsoft's Windows Terminal Server. MetaFrame incorporates Citrix's Independent Computing Architecture (ICA) protocol and provides a high-performance, cost-effective, and secure way to deploy, manage, and access business-critical applications throughout an enterprise — regardless of client device or network connection. With this innovative software, enterprises can:

- Bring server-based computing to heterogeneous computing environments and provide access to the most powerful 32-bit Windows-based applications, regardless of client hardware, operating platform, network connection, or protocol
- Offer enterprise-caliber server and client management that allows IS professionals to scale, deploy, and support applications from a single location
- Provide a seamless user experience at the desktop, delivering a wide variety of applications with exceptional performance that is independent of bandwidth

What is Server-Based Computing?

Server-based computing is a logical, efficient evolution of today's networking environments that gives organizations a way to extend resources, simplify application deployment and administration, and lower the total cost of application ownership.

With server-based computing, applications are deployed, managed, supported, and executed completely on a server. Client devices, whether "fat" or "thin," have instant access to business-critical applications on the server—without application rewrites or downloads. Because server-based computing works within the current computing infrastructure and standards, it is rapidly becoming the most reliable way to reduce the complexity and total cost of enterprise computing.

How Does Server-Based Computing Work?

Server-based computing relies on three critical components:

- A **multiuser operating system** that allows multiple concurrent users to log on and run applications in separate, protected sessions on a single server.
- A **remote presentation services architecture** capable of separating the application's logic from its user interface, so that only keystrokes, mouse clicks, and screen updates travel the network.

  MetaFrame uses Citrix's ICA, which enables virtually any client device to access virtually any application over any type of network connection. Unlike the Network Computing (NC) architecture, server-based computing does not require applications to be downloaded to client devices. As a result, application performance is neither bandwidth- nor device-dependent.
- **Centralized application and client management**, which enables enterprises to overcome the critical application deployment challenges of management, access, performance, and security.

Delivering Multiuser Computing to Windows NT Server 4.0 Environments

Microsoft developed Windows Terminal Server to offer multiuser capabilities to departments or workgroups using Microsoft Windows NT Server 4.0. This multiuser server core provides the ability to host multiple simultaneous client sessions on Microsoft Windows NT Server 4.0. MultiWin technology licensed from Citrix provides the multiuser capabilities.

To address the needs of enterprise organizations, Terminal Server requires MetaFrame and Citrix's widely endorsed ICA protocol—a *de facto* standard for server-based computing, used by more than half of the Fortune 500 companies, with over two million concurrent user licenses worldwide.

How Does Citrix MetaFrame Extend the Reach of Terminal Server?

Citrix MetaFrame brings server-based computing to the entire enterprise—including headquarters, branch offices, and remote users—and extends the capabilities of Windows Terminal Server for departmental and workgroup environments. It offers IS professionals a cost-effective way to deploy, manage, and support applications from a single point. It provides universal application access from virtually any type of client device. It ensures bandwidth-independent performance with any type of network protocol or connection, and offers unique features for enhanced application management and security.

MetaFrame provides:

- **Support for heterogeneous computing environments**
  While Terminal Server supports Windows-based devices and IP-based connections, MetaFrame goes further, providing universal access to Windows-based applications regardless of client hardware, operating platform, network connection, or LAN protocol. As a result, organizations can keep their existing infrastructures while still deploying the most advanced 32-bit Windows-based applications across the enterprise.
- **Enterprise-scale management**
  Organizations building enterprise computing solutions around Terminal Server will benefit from the robust enterprise management tools of MetaFrame, including increased system scalability and simplifed support of multiple applications for thousands of users enterprise-wide. Servers can be added easily and transparently without touching user desktops. Applications can be deployed and administered across multiple servers from a single location.

  Not only does MetaFrame provide the ability to train users of heterogeneous clients on the latest Windows-based applications, it also allows administrators to control user access to client resources, thereby maintaining system integrity and network performance. To secure corporate information, MetaFrame keeps all vital data and applications on the server, allowing it to be accessed without downloading.
- **Seamless desktop integration**
  MetaFrame goes beyond Terminal Server by offering increased functionality and enhanced user experience, including complete access to all local system resources, such as full 16-bit stereo audio, local drives, COM ports, and local printers. Applications running remotely from the server look, feel, and perform as though they are running locally. With MetaFrame, users enjoy a comfort level that eliminates the need for training and increases user productivity.

Support for Heterogeneous Computing Environments

Heterogeneous computing environments are a fact of life in the enterprise, comprising an installed base built on many client devices, operating systems, LAN protocols, and network connections. However, for the enterprise interested in making applications available to all users, there is an easy solution that enables organizations to keep their desktops of choice and still provide the best application fit for both users and the enterprise. Citrix's ICA supports all types of hardware, operating platforms, network connections, and LAN protocols. This support enables organizations to deliver the same set of applications to virtually any client device, anywhere, with exceptional performance.

- **Any client device**. Citrix MetaFrame extends the reach of Terminal Server to virtually any client device: 286, 386, 486, and Pentium computers; Windows-based terminals; Network Computers (NCs); wireless devices; ICA-based information appliances; RISC; PowerPC; and X-based devices (available through Citrix and OEM partners). All of this is done without rewriting a single line of code, changing client hardware, or adjusting client system configurations. MetaFrame also supports all types of Windows client platforms, including Windows 3.1, Windows for Workgroups 3.11, Windows 95, Windows 98, Windows NT, and Windows CE, as well as non-Windows client platforms including DOS, UNIX, Linux, OS/2 Warp, Macintosh, and Java.
- **Any network connection**. Citrix MetaFrame connects users to the network through standard telephone lines, WAN links (T1, T3, 56Kb, X.25), broadband connections (ISDN, Frame Relay, ATM), wireless and CDPD connections, and the Internet. The unique bandwidth-conserving nature of Citrix's ICA protocol makes it the ideal solution for any network type, whether Dial-up, LAN, WAN, Internet/Intranet, or even wireless networks. ICA performance is fast and consistent, regardless of network infrastructure.
- **Any network protocol**. The enterprise today consists of not only heterogeneous client devices but also heterogeneous networks. MetaFrame supports all popular LAN and WAN protocols, including TCP/IP, IPX/SPX, NetBIOS, SLIP/PPP, and asynchronous connections. MetaFrame is ideal for enterprises that need to extend bandwidth-hungry applications to users everywhere—regardless of connection type or available bandwidth—because the Citrix ICA protocol is optimized for connection speeds as low as 14.4Kbps (although 28.8Kbps is the recommended minimum speed).
- **Any application**. Users can access the full range of business and personal productivity applications including the latest Windows-based applications, client/server, mainframe, and even Java applications from a universal client, regardless of available horsepower or operating system.

Enterprise-Scale Management

MetaFrame's robust management tools help IT professionals scale systems and support multiple applications and thousands of users enterprise-wide. Servers can be added easily without having to reconfigure user systems. Applications can be administered across multiple servers from a single location—and vital data stays protected.

- **Systems management**. MetaFrame provides enterprises with greater manageability and scalability to help lower computing costs and reduce the resources needed to support users and devices. With the optional Citrix Load Balancing Services, you can group multiple MetaFrame servers into a unified *server farm*. As the size of the organization increases from dozens to hundreds or thousands of users, additional MetaFrame servers can simply be added to these farms for unlimited scalability for enterprise networks.
- **Application management**. MetaFrame enables you to manage and extend the reach of enterprise applications with tools such as Application Launching and Embedding (ALE) and application publishing. With ALE, you can extend business-critical applications across the Web while saving time and money, because there is no need to rewrite applications. With application publishing, applications can be accessed as simply as other resources on the network. You can deploy and manage multiple servers and applications from a single point.

  A new MetaFrame 1.8 feature, Program Neighborhood, gives you complete application control by publishing server-based applications into the local 32-bit Windows desktops or pushing them directly into "Start" menu programs.
- **User management**. With capabilities such as Session Shadowing and Automatic Client Update, MetaFrame enables you to monitor and support application access, troubleshoot problems, train end users, and deploy and maintain applications throughout the enterprise—all from a single location. In addition, enhanced ICA Browser management gives you control over browser parameters, such as backup ICA Browsers and ICA Gateways.

Seamless Desktop Integration

MetaFrame offers an enhanced user experience by providing complete access to all local system resources, such as disk drives, printers, ports, soundcards, and the Windows clipboard, even though applications are running remotely from the server. As a result, users need no training because they continue working in their familiar personal computing environments.

- **Local/remote transparency**. With several new MetaFrame 1.8 features, remote applications look, feel, and perform the same as local applications. Client Print Manager simplifies printer configuration, providing users with more flexibility and access to local printers. Business recovery provides reliable backup connections to ensure users have consistent access to published applications.
- **Bandwidth-independent performance**. MetaFrame is optimized for connections as low as 14.4Kbps, so every remote user can experience LAN-like application performance. This bandwidth independence improves network efficiency and, in the process, reduces network costs.

- **Universal information access**. From 16- and 32-bit applications to the latest real-time audio and video data, MetaFrame ensures you can connect to the data you need, quickly and easily. It doesn't matter if the desired information is on a local desktop, replicated database, the primary server, or a replicated server in the farm.

Who Should Use this Manual

This manual is for system administrators responsible for installing, configuring, and maintaining MetaFrame servers.

How to Use this Guide

To get the most out of the *MetaFrame Administrator's Guide*, review the table of contents to familiarize yourself with the topics discussed.

This guide contains the following sections:

Chapter	Contents
Welcome	Gives a concise summary of the features and benefits of using MetaFrame for application deployment.
Chapter 1, "Introduction"	Gives a detailed list of features and information on system sizing.
Chapter 2, "Installing MetaFrame"	Provides instructions on installing MetaFrame and upgrading from previous releases.
Chapter 3, "Citrix Licensing"	Contains information on Citrix licensing terms and requirements. Describes how to add, activate, and manage licenses.
Chapter 4, "Configuring MetaFrame"	Provides information on setting up connections and managing sessions and servers.
Chapter 5, "Publishing Applications"	Describes how to make applications and other resources available to ICA Client users.
Chapter 6, "Advanced Topics"	Contains information on advanced features, such as load balancing. Describes troubleshooting tips.
Appendix A, "MetaFrame Command Reference"	Explains how to use MetaFrame command line tools.
Appendix B, "Citrix DirectICA for MetaFrame"	Details the installation and configuration of DirectICA.
Appendix C, "ICA Browser Registry Keys"	Contains reference information on the registry keys used by the ICA Browser .

Conventions

The following conventional terms, text formats, and symbols are used throughout the printed documentation:

Convention	Meaning
Bold	Indicates boxes and buttons, column headings, command-line commands and options, icons, dialog box titles, lists, menu names, tabs, menu commands, and user input.
Italic	Indicates a placeholder for information or parameters that you must provide. For example, if the procedure asks you to type *filename*, you must type the actual name of a file. Italic also indicates new terms and the titles of other books.
ALL UPPERCASE	Represents keyboard keys (for example, CTRL, ENTER, F2).
`Monospace`	Represents text displayed at the command prompt and text file contents.
▶	Indicates a procedure with sequential steps.
•	Indicates a procedure with only one step.
▪	Indicates a list of related information, not procedural steps.
WTSRV or *%systemroot%*	Refers to the Windows Terminal Server system tree. This can be \WTSRV, \WINNT, \WINDOWS, or whatever other directory name you specified when you installed Terminal Server.
{braces}	Encloses required items in syntax statements. For example, **{ yes | no }** indicates that you must specify **yes** or **no** when using the command. Type only the information within the braces, not the braces themselves.
[brackets]	Encloses optional items in syntax statements. For example, [*password*] indicates that you can choose to type a *password* with the command. Type only the information within the brackets, not the brackets themselves.
| (vertical bar)	Stands for "or" and separates items within braces or brackets. For example, **{ /hold | /release | /delete }** indicates that you must type **/hold** or **/release** or **/delete**.
… (ellipsis)	Indicates that you can repeat the previous item(s) in syntax statements. For example, **/route:***devicename*[,…] indicates that you can specify more than one device, putting commas between the device names.

Finding More Information About MetaFrame

Your MetaFrame package includes the following printed documentation:

- The CD liner notes includes an overview of the product, Citrix support information, and instructions for activating your Citrix software licenses.
- The *MetaFrame Administrator's Guide* tells administrators how to install, configure, and maintain MetaFrame servers.
- The *Citrix ICA Client Quick Reference Cards* give users step-by-step instructions for using the Citrix ICA Clients to connect to Citrix servers and run published applications.

Your MetaFrame software includes the following online documentation in WinHelp format in the MetaFrame Books Online:

- The *MetaFrame Solutions Guide* gives administrators detailed information about planning, deploying, and configuring server-based computing solutions using MetaFrame, the Citrix ICA Clients, and a wide variety of third-party hardware and software.
- The *Citrix ICA Client Administrator's Guides* tell administrators how to install, configure, and deploy the various ICA Clients to end-users.
- The online version of the *MetaFrame Administrator's Guide.*

To access *MetaFrame Books Online*, click **MetaFrame Books Online** in the **MetaFrame Tools** folder.

All of the documentation for MetaFrame is also available in Adobe PDF format in the documentation directory of your MetaFrame CD-ROM. Using the Adobe Acrobat Reader, you can view and search the documentation electronically or print it for easy reference. To download the Adobe Acrobat Reader for free, please go to Adobe's Web site at http:\\www.adobe.com.

Important Please consult the Readme.txt file in the root directory of your MetaFrame CD-ROM, for any last-minute updates, installation instructions, and corrections to the documentation.

Finding Information About Windows NT Server, Terminal Server Edition

Most Terminal Server compatibility guidelines can be applied to Citrix MetaFrame because MetaFrame is designed to run with Terminal Server. For example, MetaFrame supports the deployment of Win32, Win16, DOS, OS/2 1.x (text only), and POSIX applications. The ICA technology included in MetaFrame extends the capabilities of Windows NT and, in some cases, requires additional setup and configuration for best application performance.

For Terminal Server compatibility information, see the following Microsoft resources:

- The Microsoft Web site, http://www.microsoft.com
- Microsoft Technet

For instructions on installing and using Terminal Server, see the Microsoft documentation included in your Terminal Server package.

Citrix on the World Wide Web

Citrix offers online Technical Support Services at http://www.citrix.com that include the following:

- Downloadable Citrix ICA Clients, available at http://download.citrix.com
- A Frequently Asked Questions page with answers to the most common technical issues
- An FTP server containing the latest service packs and hotfixes for download
- An Online Knowledge Base containing an extensive collection of technical articles, troubleshooting tips, and white papers
- Interactive online support forums available as HTML pages and as a list server

CHAPTER 1

Introduction

Overview

This chapter introduces Citrix MetaFrame Application Server for Windows. Topics in this chapter include:

- Citrix MetaFrame Features
- The Citrix ICA Clients
- System Sizing
- ICA Overview

Citrix MetaFrame Features

- **Enterprise scalability**. Terminal Server can accommodate up to 60 concurrent users on a single four-processor SMP Pentium server, depending on the application mix. Multiple MetaFrame servers can be combined into a server farm that utilizes load balancing to increase capacity as needed.
- **Extensive connectivity**. MetaFrame can connect users through standard telephone lines, ISDN lines, wide-area network (WAN) links, broadband connections, corporate Intranets, or the Internet. ICA connections can be made over TCP/IP, NetBIOS, IPX, and SPX protocols, allowing you to access your MetaFrame server over a LAN, WAN, or RAS connection. Dial-In async support eliminates the need to configure a RAS server or RAS on client computers.
- **Flexible management and administration**. Server-based system administration makes configuration, problem identification, and problem resolution quick and efficient. MetaFrame includes an extensive set of end-to-end Windows management tools that allow Citrix servers and remote users to be configured, administered, monitored, and supported from anywhere.
- **Automatic client update**. The automatic client update feature makes distributing the latest version of the Citrix ICA Clients to client computers an almost effortless job. Simply install the latest version of the client software on the server, then schedule the download and installation of that software to client devices. For more information, see the *Citrix ICA Client Administrator's Guides* for the clients you plan to deploy.
- **Remote node compatibility**. MetaFrame can be used with most popular third-party remote node hardware and software to significantly boost the performance of LAN-resident applications.
- **Application publishing support**. MetaFrame supports application publishing. A *published application* contains all of the information needed to launch an application on a Citrix server and can be used with Citrix load balancing support. See Chapter 5, "Publishing Applications" of this manual for more information about application publishing.
- **Enhanced security features**. MetaFrame supports enhanced security utilities and procedures that help you protect your system from unauthorized access. To protect sensitive data, MetaFrame incorporates multilevel system security and optional data encryption add-ons.
- **Configurable TCP/IP port setting for ICA protocol**. This feature lets you configure Citrix ICA packets to be compatible with many popular TCP/IP firewall products.

- **Load balancing support**. With load balancing, MetaFrame servers can be logically pooled in a *server farm*. When a user launches a published application that is configured for load balancing, the load balancing support routes the application to the most lightly loaded server in the farm for execution. You can create a farm of servers that run predefined applications. The load determination criteria for any server in the farm can be fine-tuned from any server in the farm. You can view and manage user sessions, regardless of which server in the farm is hosting the session. Both MetaFrame and *WINFRAME* servers can join the same server farm.

  Note Each Citrix server that will support load balancing must have Citrix Load Balancing Services installed.

- **Activation code-based licensing**. MetaFrame uses the Citrix serial number/activation code licensing scheme. Every licensed Citrix product (Citrix server software or server extension) has an associated *serial number*. When you install the software, you enter the product's serial number. You must then register the license number with Citrix to get an *activation code*. Use the Citrix Licensing utility to activate your software by entering the code..

  See Chapter 3, "Citrix Licensing," for information on how to activate your MetaFrame server software. **You must activate your MetaFrame software after installing it**.

- **ICA Client Creator**. Use the ICA Client Creator to create diskettes containing the following Citrix ICA Clients: DOS, Win16, Win32, and Web. See the *Citrix ICA Client Administrator's Guides* for those clients.

- **Web computing support**. MetaFrame supports Web computing features that let you publish applications on your corporate Intranet or the Internet. From a single point, administrators and Webmasters can publish an application, automatically generate ALE HTML code, and deploy the application for use throughout the local or extended enterprise. Users simply point their browsers to an Internet or Intranet page, where they can access Windows-based applications regardless of their physical location.

  The Citrix ICA Windows Web Clients can be used with any Windows Web browser to support launched applications. When used with Microsoft Internet Explorer or Netscape Navigator, applications can be embedded within Web pages. Firewall support lets you interpose firewalls between your MetaFrame server and the Internet for increased security. See the *Citrix ICA Client Administrator's Guide* for the Citrix ICA Web Clients for more information.

New in This Release

- **Program Neighborhood**. Program Neighborhood introduces a new metaphor for user application access that replaces Remote Application Manager for the Citrix ICA Win32 Client and delivers access to centrally deployed applications. With the introduction of Program Neighborhood, server-based applications can now be pushed to the Program Neighborhood client, integrated into the local 32-bit Windows desktop, or pushed directly to the client's Start menu.

  Similar in concept to Windows Network Neighborhood, Program Neighborhood provides total administrative control of applications by providing users with dynamic access to published applications. Not only do users have an enhanced server-based application experience, but also no client configuration is required. Program Neighborhood provides complete administrative control over application access and local desktop integration.

- **SpeedScreen**. SpeedScreen builds on the intelligent agent technology, introduced in MetaFrame 1.0, that reduces the transmission of frequently repainted screens. In comparison with MetaFrame 1.0, bandwidth consumption is reduced, on average, by 25-30% and total packets transmitted is cut by up to 60%, resulting in significant improvements in measured speed on restricted bandwidth connections.

  SpeedScreen furthers the user experience with consistent performance regardless of network connection by reducing latency and improving the feel of the server-based application.

- **Installation Management Services (IMS) Ready**. The Installation Management Services option gives Citrix administrators the ability to centrally manage software replication across Citrix server farms. You can run an application's installation routine just once per platform, then deploy the application to each server in the farm automatically.

  This innovative system services option for MetaFrame offers administrators an excellent alternative to manually installing and configuring the same application on multiple Citrix servers. Administrators can now more easily and cost-effectively deploy applications to thousands of users across the enterprise.

- **Video Ready**. VideoFrame in conjunction with MetaFrame 1.8 enables the production and deployment of custom video applications to 32-bit Windows ICA Clients using an innovative intelligent compression and a streaming extension to the ICA protocol.

  By integrating VideoFrame into a Citrix server farm, administrators can now deploy custom video applications to any 32-bit Windows desktop, on demand, while maintaining consistent performance across any network connection, regardless of available bandwidth.

- **ICA Browser Management**. With ICA Browser management, part of the enhancements to Citrix Server Administration, administrators now have the ability to control browser parameters such as backup ICA Browsers, ICA Gateways, and update and refresh intervals. Administrators can also configure which servers always attempt to become the master ICA Browser.

  ICA Browser management simplifies browser administration through an intuitive user interface for better system scaling and management.
- **License Pool Recovery**. Citrix has introduced a new backup licensing feature to better manage pooled licenses across the server farm. With this feature, you can define the number of backup servers to which user licensing data is replicated.

  This new addition to Citrix license pooling provides a greater level of fault tolerance across multiple Citrix servers.
- **Client Device Licensing**. This new feature allows a user to establish multiple sessions to multiple servers while consuming only a single pooled license for each session.

  Client device licensing reduces IT organizations' total cost of ownership (TCO) by providing seamless access to multiple applications across multiple servers, without incurring additional licensing costs.

The Citrix ICA Clients

The Citrix ICA Clients allow users to connect to Citrix servers and access applications. This manual gives you instructions for configuring MetaFrame servers. For detailed instructions on installing and configuring Citrix ICA Clients, see the *Citrix ICA Client Administrator's Guides* for the clients you plan to deploy.

Citrix ICA Client Platforms

Versions of the Citrix ICA Client are provided for many popular computing platforms, including:

- The Citrix ICA Client for DOS. Use this client for DOS 3.3 or later. There are two versions of the ICA DOS Client, 16-bit and 32-bit. The 32-bit version provides more features than the 16-bit version, while requiring less conventional memory.
- The Citrix ICA Client for Win16. Use this client for Windows Version 3.1 or Windows for Workgroups 3.11. This version of the ICA Client is also supported on OS/2 Version 2.1, OS/2 Warp Connect Version 3.0, and OS/2 Warp Version 4.0.
- The Citrix ICA Client for Win32. Use this client for Windows NT 3.51, Windows NT 4.0, MetaFrame, *WINFRAME*, and Windows 95/98.

- The Citrix ICA Client for Macintosh. Use this client for 68030/040 and PowerPC-based Apple Macintosh computers.
- The Citrix ICA Client for UNIX is available in the following versions:
  - Linux RedHat 5.0 and above
  - SCO UnixWare 7 (UnixWare 2.1 and OpenServer 5 with the Binary Compatibility Module from SCO)
  - Hewlett Packard HP-UX 10.20 and above
  - Sun Solaris 2.5.1 and above
  - Sun SunOS 4.1.4
  - Silicon Graphics IRIX 6.3 and above
  - Digital UNIX 3.2 and above
  - IBM AIX 4.1.4 and above
- The Citrix ICA Windows Web Clients support application launching with Windows-based Web browsers that support configurable MIME types. Many Web browsers also support application embedding, including Microsoft Internet Explorer and Netscape Navigator.
- The Citrix ICA Client for Java supports application embedding with Web browsers that fully implement Java Virtual Machine (JVM) Version 1.1 or greater.

Citrix continually updates its support for client platforms and versions. See the Citrix Web site for information on new ICA Clients. For more information on supported platforms, see the *Citrix ICA Client Administrator's Guides* for the clients you plan to deploy.

Citrix ICA Client Features

- **TAPI support for Win32 Clients**. The ICA Win32 client now provides TAPI support for dial-up connections. Users no longer need to manage separate modem entries for their local communications programs and the ICA Client.
- **TAPI emulation for DOS and Win16 Clients**. Citrix ICA Clients for DOS and Win16 can now reap the benefits of today's state-of-the-art modems by interpreting Windows 95/Windows NT modem configuration files into legacy .ini files to ensure optimum performance for dial-up users.
- **International keyboard support for Web Clients**. Users worldwide can exploit the benefits of Citrix ICA Clients for Internet Explorer and Netscape Navigator, both of which now support international keyboard layouts.
- **256 color DOS Client support**. No longer are DOS ICA Client users limited to just 16 colors. With this new enhancement, users can enjoy the quality and richness of 256 color applications and graphics on legacy DOS devices.

- **Low bandwidth requirements**. The highly efficient Citrix ICA protocol typically uses a maximum of 20K of bandwidth for each session.
- **Local/Remote transparency**. Easy to use, all-purpose remote connectivity over a single remote connection eliminates the user dilemma of having to choose between remote node or remote control for running various applications.
- **Client printer and disk drive mapping**. Users who access a MetaFrame server with the Citrix ICA Client can transparently access their local printers and disk drives (fixed and removable). The drive letters used for drive mapping are configurable and long filenames are supported.
- **Automatic client printer mapping**. Any printers detected when you connect to a Citrix server are automatically added to the Print Manager. Client printers can be browsed and connected to in the same way as network printers (Windows clients only).
- **COM port mapping**. The ICA Client COM port redirector gives Citrix ICA DOS, Win16, and Win32 client users access to virtually any peripheral that requires a COM port for operations. COM port mapping is similar to printer and drive mapping, and allows users to access a COM port on the client computer as if it were connected to the Citrix server.
- **Windows clipboard integration**. Users can cut and paste data between ICA sessions and local applications using the Windows clipboard (Windows clients only).
- **Remote audio**. MetaFrame introduces remote audio support for the Citrix ICA DOS, Win16, and Win32 clients. Compression can be used to maximize bandwidth utilization. Audio support requires a Sound Blaster Pro-compatible sound card in the ICA Client computer.
- **Disk caching and data compression**. These can be used to increase performance over low speed asynchronous and WAN connections. *Disk caching* stores commonly used portions of your screen (such as icons and bitmaps) locally, increasing performance by avoiding retransmission of locally cached data. *Data compression* reduces the amount of data sent over the communications link to the client computer.
- **Simplified remote application launching**. You can create a remote application entry to connect to a Citrix server or to a published application that contains all of the information necessary to launch a user session or an application. All the user needs to do is double-click on the application entry's icon on the desktop.

- **Seamless Windows support**. The Citrix ICA Win32 Client now supports the seamless integration of local and remote applications on the local Windows 95 or Windows NT 4.0 desktop. By simply selecting the **Seamless Windows** option when configuring a connection to a MetaFrame server, a user no longer needs to access an entire remote desktop to run remote Windows applications. With a single session a user can gain access to multiple applications, have fully functional local keyboard controls (such as ALT+TAB), switch between local and remote applications on the local taskbar, define remote application icons on the local desktop, and even tile and cascade between local and remote Windows applications. These new features of the Citrix Win32 ICA Client fully integrate local and remote applications to provide a true seamless user experience.
- **Business Recovery Client**. The Citrix ICA Client now includes the additional intelligence to support multiple sites (such as a primary and hot backup) with different addresses for the same published application name.

  This feature provides for consistent connections to published applications in the event of a primary server disruption. Users now have an even higher level of fault tolerance and seamless user experience.
- **Client Print Manager**. This client printing enhancement allows users to define which client printers can be configured on their client devices. It provides a means to store printer properties on a per-client-device basis while simplifying printer configuration for non-Windows clients.

  This new feature provides for an even higher level of seamless experience, giving users additional flexibility and access to local system resources.

These features are not available on all ICA Clients. For detailed information on supported features, see the *Citrix ICA Client Administrator's Guides* for the clients you plan to deploy.

System Sizing

MetaFrame supports multiple users on a Windows Terminal Server. A multiuser system requires more system resources than a single-user system. This section contains some system sizing guidelines that can help you decide on a hardware configuration that will support your users with optimal performance.

Most companies find that their users can be placed in one of two categories: typical users and power users. A *typical user* generally uses one or two applications but normally only one at any given time. Little actual program data is transferred between the client and server, and the users rarely use Object Linking and Embedding (OLE). A *power user* is a more sophisticated user who uses three or more applications, often with several active at the same time. Data is often cut-and-pasted between local and remote applications, and OLE is used heavily.

Obviously, power users consume more resources than typical users; this must be factored in when configuring MetaFrame servers. A good rule of thumb is that one power user is equivalent to two typical users in processor utilization and memory requirements. All the configuration examples in this section are based on numbers of typical users; adjust them according to the number of power users anticipated.

Processor, Bus Architecture, and Memory Requirements

The processor and bus architecture are fundamental to MetaFrame server performance. The ISA (AT bus) architecture is low-bandwidth and is not recommended for MetaFrame servers. Use a higher-performance bus, such as EISA or PCI for best performance. All of these buses support the high sustained data transfer rates typical of a MetaFrame server.

The memory requirements for MetaFrame and Windows Terminal Server are 16MB of RAM, plus 4MB for each typical user or 8MB for each power user. In many cases, adding RAM has a larger effect on system performance than upgrading to a faster processor.

It is important to note that the processor and memory requirements for MetaFrame scale linearly. This means you can roughly double the number of users supported on a multiprocessor-capable system by doubling the number of processors and doubling the amount of RAM memory. For this reason, purchase a multiprocessor-capable system, even if you initially purchase only one processor, to allow for convenient system scaling as your requirements grow. Note that not all multiprocessor systems scale the same way because of bus differences. The bus architecture in a multiprocessor system is crucial for multiprocessor performance with more than four processors, and vendor-specific drivers are usually required.

Some sample configurations and supported user counts (for typical and power users) follow:

Processor	Memory (MB)	Typical users	Power users
Pentium Pro 200MHz	128	32	16
Pentium Pro 200MHz	256	64	32
Dual-Processor Pentium Pro 200MHz	512	120	60

Other Peripherals

Besides the system processor and memory, the hard disk is an important factor in system throughput. SCSI disk drives and adapters, especially Fast SCSI and SCSI-2 compatible devices, have significantly better throughput than ST-506, IDE, or ESDI disk drives and adapters.

For the highest disk performance, you may want to consider using a SCSI RAID controller. RAID (Redundant Array of Independent Disks) controllers automatically place data on multiple disk drives and can increase disk performance and improve data reliability. More information about RAID can be found in the *MetaFrame Solutions Guide.*

The ICA protocol is highly compressed and causes negligible loading on a network, but because the MetaFrame server handles all network requests, a high-performance network interface card (NIC) is recommended.

If a multiport asynchronous communications adapter is installed for supporting serial ICA connections, be sure to use an intelligent (microprocessor-based) adapter to reduce interrupt overhead and increase throughput.

16-Bit Versus 32-Bit Applications

Windows NT is a Win32 (32-bit) environment and Windows 3.x for DOS is a Win16 (16-bit) environment. Windows NT runs Win16 applications through a process called WOW (Win16 on Win32), translating 16-bit applications in enhanced mode. This process causes Win16 applications to consume additional system resources, which reduces the number of users per processor by 20% and increases the memory required per user by 25%. For this reason, Win32 versions of applications should be used whenever possible. If you intend to run Win16 applications, adjust your processor and memory requirements accordingly.

Using Performance Monitoring Tools

Use the performance monitoring tools supplied with Windows Terminal Server to monitor system performance and the effects of configuration changes on system throughput. The most important measurements for performance monitoring are the percentage of total processor time, memory pages per second , percentage of network utilization, and hard disk I/O rates.

A good way to estimate how many users a server can support is to measure system performance with two to five users on the system and then scale the results. This method has been found to yield reliable results.

ICA Overview

MetaFrame provides server-based computing to local and remote users through its advanced Independent Computing Architecture (ICA) protocol. When you use MetaFrame, applications are loaded and executed on the MetaFrame server. As the application runs, the MetaFrame server intercepts the application's display data and uses the ICA protocol to transmit this data to the Citrix ICA Client running on the user's device. Similarly, the ICA Client sends keyboard and mouse data to the MetaFrame server for processing.

The Citrix ICA protocol provides the following advanced capabilities:

- Transparent support for off-the-shelf Windows and DOS applications
- High performance on high- and low-bandwidth connections
- Minimal client workstation requirements
- Full-screen text presentation
- Keyboard and mouse input with data compression
- Error detection and recovery
- Encryption
- Data compression
- File system redirection for client drive mapping
- Print redirection for client printer mapping
- COM port redirection
- Clipboard cut-and-paste support (Windows clients only)
- Audio support
- Intelligent caching of bitmaps
- Persistent caching to disk
- Advanced algorithms that discard redundant screen changes and optimize display operations

Client drive mapping allows drive letters on the Citrix server to be redirected to drive letters that exist on the client computer.

Client printer mapping allows a printer device on the Citrix server to be redirected to a printer on the client computer.

Client COM port mapping allows a COM port on the client computer to be treated as a COM port on the Citrix server.

Audio support allows application sounds and .wav files to be played on the client computer.

Configuration of these mappings is built into the standard Windows NT device redirection facilities. The client mappings appear as another network that presents the client devices as sharepoints to which a drive letter or printer port can be attached.

CHAPTER 2

Installing MetaFrame

Overview

This chapter describes how to install Citrix MetaFrame on a Windows Terminal Server computer. Terminal Server must already be installed and configured before MetaFrame is installed. See “System Sizing” in Chapter 1 for hardware and software requirements for Citrix MetaFrame.

The topics in the chapter include:

- Before You Begin
- Upgrading to MetaFrame 1.8
- Installation
- Configuring a Modem
- Running Setup in Unattended Mode

Before You Begin

Please make sure you read the following information before installing MetaFrame.

- You must have Windows NT Server, Terminal Server Edition installed before you can install Citrix MetaFrame.
- All network protocols (TCP/IP, IPX, NetBIOS) that will be used for ICA connections must already be configured in Terminal Server. See the Windows NT documentation for instructions on configuring network protocols.
- If you have modems already configured for use with Windows NT Remote Access Service (RAS) that you want to configure for ICA Dial-In connections, remove them from the RAS modem pool before starting MetaFrame installation.
- If you have a multiport async adapter, install it before starting MetaFrame installation. You can choose to install modems connected to the multiport adapter before or during MetaFrame installation.

Warning The master ICA Browser election criteria has changed in this release. The version number of the ICA Browser is the highest criteria and overrides an ICA Browser specifically configured in the registry as the master ICA Browser.

If you have designated a fixed (hard-coded) master ICA Browser in an existing Citrix server farm, install MetaFrame 1.8 on the master ICA Browser machine first. If you install MetaFrame 1.8 on another server first, that server will become the master ICA Browser.

The Citrix Server Administration option that prevents a MetaFrame 1.8 server from becoming the master ICA Browser also disables certain MetaFrame 1.8 features.

Drive Mapping and Server Drive Reassignment

Client drive mapping allows remote users to transparently access their local drives when logged on to a MetaFrame server. If the MetaFrame server drive letters do not conflict with client drive letters, the client drives can be accessed with their existing drive letters.

Client drive letters that conflict with server drive letters are mapped to drive letters starting with V and working backwards. The server floppy disk drives are not available to users, so client floppy disk drives are always mapped to their existing drive letters. By default, user sessions have the following drive mappings:

Drive letter	Is accessed from the ICA session as:
Client Drives:	
A	A
B	B
C	V
D	U
Server Drives:	
C	C
D	D
E	E

If you do not want the MetaFrame server drive letters to conflict with the client drive letters, the server drive letters can be reassigned to higher drive letters. If the server drives are reassigned, user sessions have the following drive mappings:

Drive letter	Is accessed from the ICA session as:
Client Drives:	
A	A
B	B
C	C
D	D
Server Drives (after reassignment):	
M	M
N	N
O	O

You can do this during MetaFrame Setup or after MetaFrame has been installed. See “Reassigning Server Drives” in Chapter 4 for instructions on changing the server drive assignments after installation.

Important If you intend to remap the server drive letters, install MetaFrame and remap the server drive letters before installing any applications.

If you remap the server drive letters, the following registry keys are searched and all drive references changed to reflect the new drive letters:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft*
HKEY_LOCAL_MACHINE\SOFTWARE\Classes*
HKEY_LOCAL_MACHINE\SOFTWARE\Equinox\eqn\CurrentVersion \NetRules

HKEY_LOCAL_MACHINE\SYSTEM*
HKEY_CLASSES_ROOT*
HKEY_USERS*

The pagefile entry and the following shortcut files are also updated:

%SystemRoot%\Profiles\Default User*.lnk
%SystemRoot%\Profiles\Administrator*.lnk
%SystemRoot%\Profiles\All Users*.lnk

The first time a user logs in to the MetaFrame server after you remap drives, references to the old drive letters in the user's profile are updated.

Upgrading to MetaFrame 1.8

The following versions of MetaFrame and *WINFRAME* can be upgraded to MetaFrame 1.8:

- MetaFrame 1.0
- *WINFRAME* 1.6 with Service Pack 5
- *WINFRAME* 1.7

In addition to the settings that Terminal Server preserves on upgrades, the following MetaFrame 1.0 and *WINFRAME* information is preserved:

- Server drive assignments
- All ICA connection (previously WinStation) configurations
- All Citrix licenses (licenses are preserved to allow MetaFrame 1.8 upgrade licenses to be applied after the upgrade)

  Note After upgrading, apply and activate your upgrade license.

- Published applications
- ICA Gateway configuration

This information is retained for use when you install MetaFrame. MetaFrame Setup detects the retained information and uses it to configure the MetaFrame system.

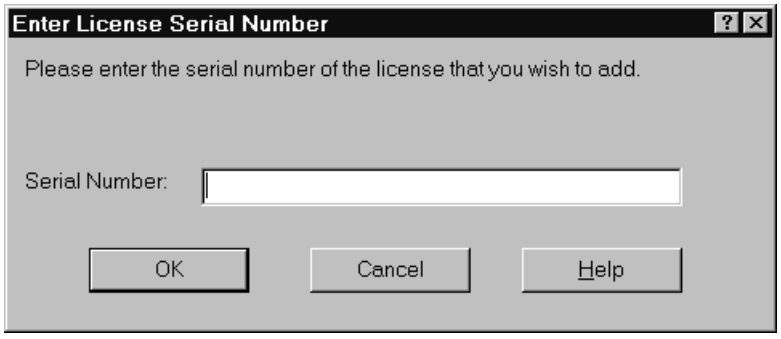
Note SecureICA for *WINFRAME* 1.7 is not preserved. You must obtain the version of SecureICA Services for this release.

Installation

▶ **To install Citrix MetaFrame**

1. Log on to the Windows Terminal Server console as an administrator.
2. Insert the MetaFrame CD in the server's CD-ROM drive. If your CD-ROM drive supports Autorun, the MetaFrame CD-ROM installation splash screen automatically appears.

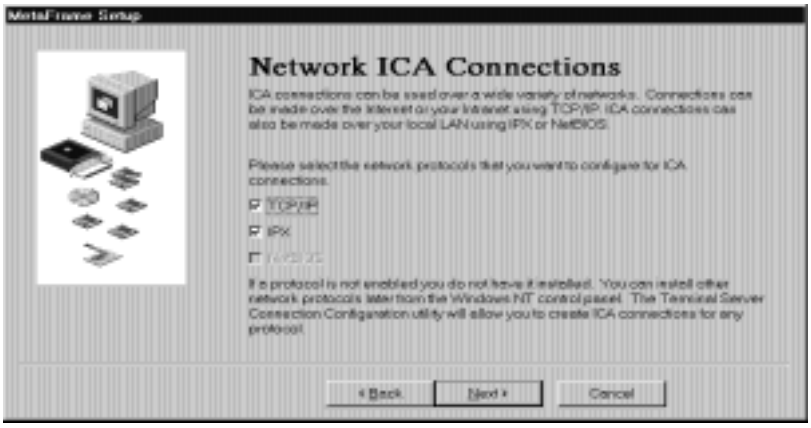
   If the splash screen does not automatically appear, from the **Start** menu, click **Run** and type ***d*:\i386\autorun.exe** where *d* is the letter of your CD-ROM drive.
3. Click **MetaFrame Setup** to begin installation.
4. Verify that no other programs are running and click **Next**. The **Setting Up MetaFrame** dialog box appears.
5. Click **Next**. Setup copies files to your hard disk and makes changes to your system.
6. When copying is complete, the **MetaFrame 1.8 Licensing** dialog box appears. Click **Add License Packs** to enter your product serial number.
7. The MetaFrame Licensing **Enter License Serial Number** dialog box appears. Enter your license number **exactly** as it appears on the license sticker on your CD case and click **OK**.



8. A message appears reminding you to activate your license when installation is completed. Click **OK** after you have read the message.
9. If you have additional Citrix licenses to install (for example, Load Balancing Services), click **Yes** to install another license and repeat Steps 7 and 8. When you have finished installing all the licenses for this server, click **No** and then click **Next** when you return to the **Licensing** dialog box.

   See Chapter 3, "Citrix Licensing," for a complete description of Citrix licensing.

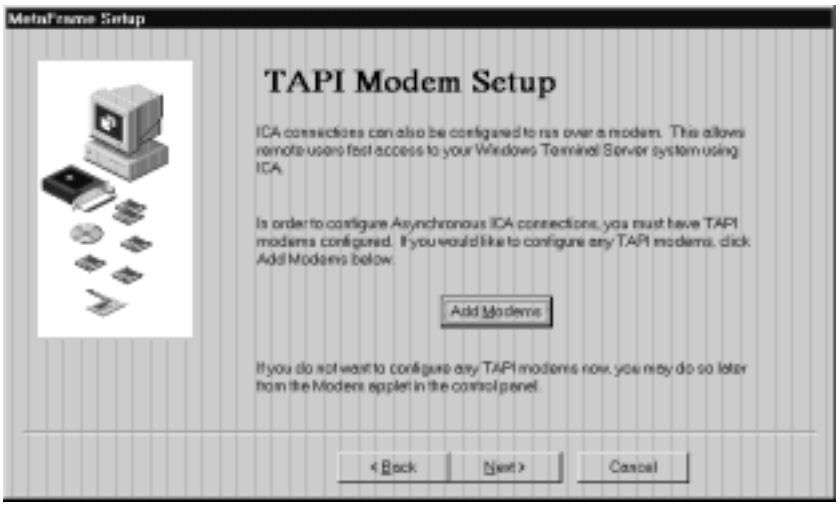
10. The **Network ICA Connections** dialog box appears. Select all the network protocols this server will use for ICA connections (TCP/IP, IPX, and NetBIOS). Click **Next** to continue.



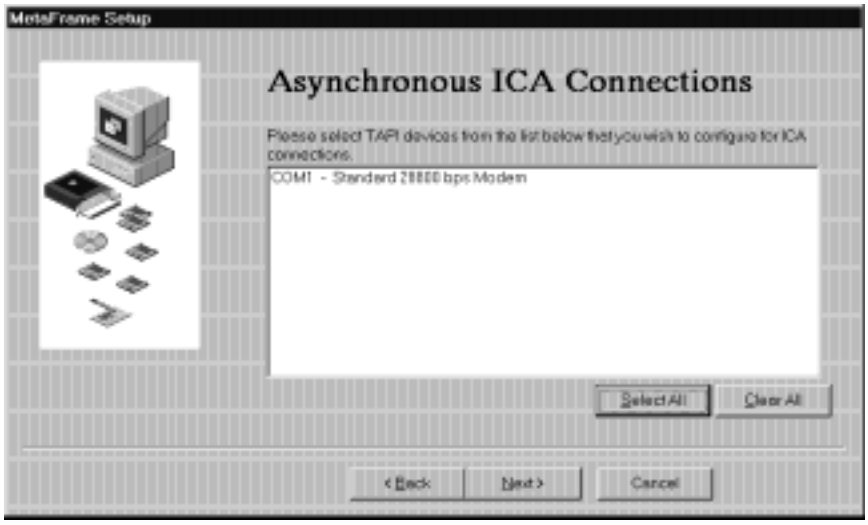
By default, ICA connections are created for all protocols already configured in Terminal Server. If you need to configure additional ICA connections after MetaFrame installation, see Chapter 4, “Configuring MetaFrame,” for more information.

11. The **TAPI Modem Setup** dialog box appears.

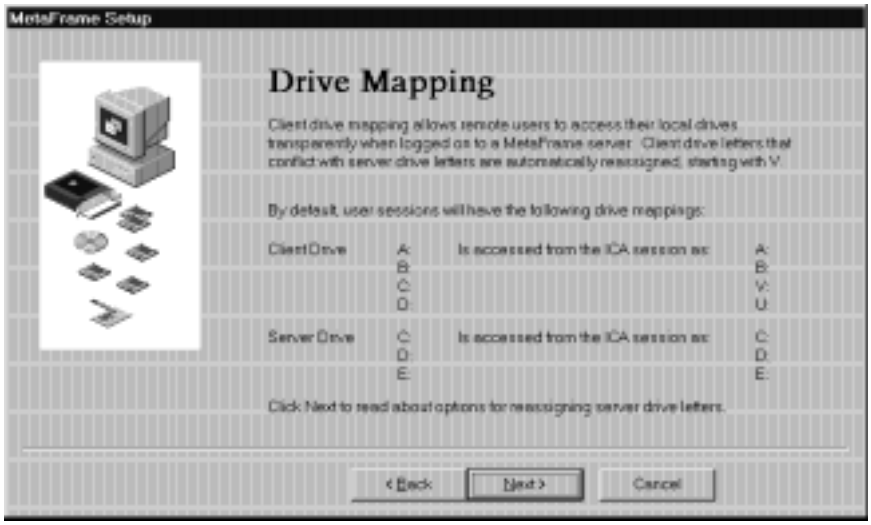
Before a modem can be used by Windows NT, it must be installed. This process is normally done during Windows NT installation, but can also be done during MetaFrame installation. To add or configure modems, click **Add Modems**. See “Configuring a Modem” later in this chapter for detailed instructions on adding a modem.



12. If TAPI devices are installed, the **Async ICA Connections** dialog box appears. Select the devices to configure for dial-in ICA connections. Click **Next** to continue.



13. If the server drives are not already reassigned (that is, the C drive letter is assigned to a hard drive), the **Drive Mapping** dialog box appears.



Note Please read the "Drive Mapping and Server Drive Reassignment" section of this chapter and the information displayed in this dialog box carefully before clicking **Next**.

This process is not reversible and should be well understood before continuing.

14. The **Server Drive Reassignment** dialog box appears.

Note Please read the "Drive Mapping and Server Drive Reassignment" section of this chapter and the information displayed in this dialog box carefully before clicking **Next**.

If you decide to reassign the server drive letters, select the **Remap the server drives** check box and specify a starting drive letter. Click **Next** to continue.

15. When Setup is complete, the **System Reboot** dialog box appears. Remove the MetaFrame CD-ROM and click **Finish** to reboot.

Configuring a Modem

Follow the steps below if you clicked **Add Modems** in Step 11 of the MetaFrame installation procedure.

1. If no modems are already configured in your system, the **Install New Modem** dialog box appears. If you already have modems configured, proceed to Step 8.
   - If you want to auto-detect your modem, click **Next**.
   - If you want to manually select your modem, select the **Don't detect my modem** check box and click **Next**. Proceed to Step 4.

2. If you have a multiport async adapter, select a port on which to run auto-detection. MetaFrame Setup auto-detects the modem connected to the specified port. You can configure multiple ports with the same modem type in Step 5 below.
3. Windows NT searches for your modem. The detected modem is displayed. If this is the correct modem type, click **Next** and proceed to Step 5.

   —Or—

   If you want to select another modem type, click **Change**.

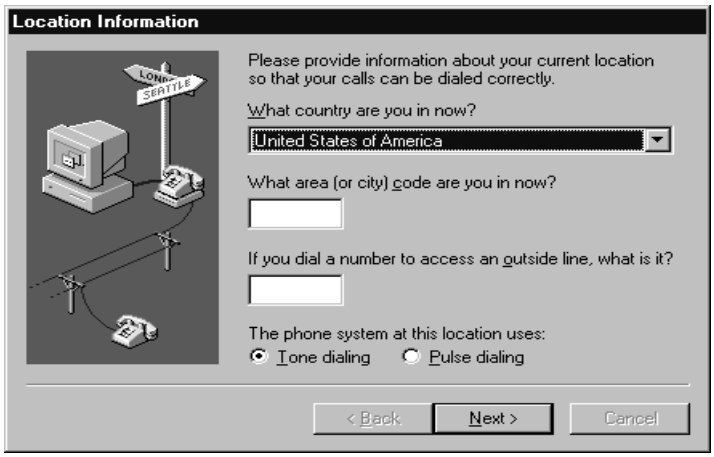
   —Or—

   If no modem is detected, click **Next**.
4. Select the proper manufacturer and model of your modem and click **Next**.

   If you do not see your modem on the list, select a similar model from the same manufacturer or a generic modem type.

   —Or—

   If your modem came with a driver on disk, click **Have Disk** and follow the manufacturer's instructions for installing the driver.
5. The port selection dialog box appears. Select the port(s) to which the modem is connected. Click **Next** when finished.
6. If this is the first modem installed, the **Location Information** dialog box appears.



   Specify the country you are in, the area or city code, the number that must be dialed to reach an outside line, and whether the modem should use tone or pulse dialing. These settings are used with all modems. When finished, click **Next**.
7. A dialog box appears informing you that the modem has been set up successfully. Click **Finish**.

8. The **Modems Properties** dialog box appears.

To change the configuration of an existing modem, select the modem and click **Properties**. To add another modem, click **Add** and repeat Steps 1 through 5. When you are finished, click **Close** and then click **Next** in the **TAPI Modem Setup** dialog box.

Running Setup in Unattended Mode

Use unattended setup to install or upgrade MetaFrame without operator intervention.

Unattended setup uses an optional *answer file* to provide answers to the questions asked during Setup. If you do not use an answer file, or if you use an answer file but do not specify answers to some questions, default answers are used for those questions.

The default answers used are:

- No licenses are added
- ICA connections are configured for all network protocols already configured in Terminal Server
- Asynchronous ICA connections are configured for all modems already configured in the Modems control panel
- Server drives are not reassigned

▶ **To perform an unattended installation or upgrade**

1. Insert the MetaFrame CD-ROM in the CD-ROM drive of the Terminal Server computer, or insert the MetaFrame CD-ROM in a CD-ROM drive accessible over the network. If your CD-ROM drive supports Autorun, the **MetaFrame CD-ROM** start window automatically appears. Close the start window.
2. Choose **Run** from the **Start** menu and type

   ***d*:\i386\setup /u[:*answer_filename*]**

   where *d* is the drive letter of your CD-ROM drive and *answer_filename* is the name of the optional answer file.
3. Read the MetaFrame server license and click **OK** if you agree to the terms.

Answer File Syntax

There are four sections in the MetaFrame answer file. Each section is enclosed in square brackets.

- The **License Serial Numbers** section. This section contains the Citrix MetaFrame base license and server extension license serial numbers with an appended equal sign (=). Enter the license numbers exactly as they appear on the serial number sticker provided with your software. You can specify multiple licenses in the answer file. The licenses are added in the order they are listed in the answer file.

  Important You must list your base license first.

- The **ICA Network Protocols** section. This section specifies if ICA connections are to be configured for the specified protocols (TCP/IP, IPX, and NetBIOS).

  The options are:

  TCP=yes | no

  IPX=yes | no

  NETBIOS=yes | no

- The **Drive Reassignment** section. This section specifies if the drive letters on the MetaFrame server are to be reassigned, and if yes, what the new drive letter for the server drive C is to be.

  ReassignDriveLetters=yes | no

  NewDriveLetter=*driveletter*

- The **Options** section. This section contains additional options for unattended setup. The reboot option specifies MetaFrame Setup shuts down and restarts the server machine after setup completes.

  RebootOnFinish=yes | no

A Sample Answer File

Here is a sample answer file that performs the following actions during MetaFrame Setup:

- Installs two licenses (a base license and a server extension license)
- Configures ICA connections for the TCP/IP, IPX, and NetBIOS protocols
- Reassigns the server drive C to drive M

```
[License Serial Numbers]
CTX-0000-0000-0000-000000=
CTX-0000-0000-0000-000000=

[ICA Network Protocols]
TCP=yes
IPX=yes
NETBIOS=yes

[Drive Reassignment]
ReassignDriveLetters=yes
NewDriveLetter=M

[Options]
RebootOnFinish=Yes
```

CHAPTER 3

Citrix Licensing

Overview

This chapter explains Citrix licensing. Topics in this chapter include:

- What is Citrix Licensing?
- The Citrix Licensing Program
- Getting an Activation Code

What is Citrix Licensing?

Citrix licensing is separate from Microsoft licensing. There are two types of Citrix licenses:

- **Base licenses**. The base license enables the multiuser features of your Citrix server and can include a user count. If the base license is not present, ICA connections are not supported and server extension licenses cannot be added. Every Citrix server comes with a base license.
- **Server extension licenses**. Citrix server extension licenses increase the user count or enable additional functionality, such as load balancing.

You must activate each Citrix license to complete the installation of your software. Some licenses have a grace period after installation, where they will work for a time with periodic reminder messages. If the license is not activated during the grace period, the license is automatically disabled at the end of the grace period.

To activate a Citrix license you use three numbers:

serial number	The number on your CD case that you enter during setup.
license number	The serial number appended with a code that makes it unique to this server.
activation code	A number that validates and enables a Citrix license.

Understanding User Counts

Base licenses and user licenses come with a user count. A server's *user count* is the number of ICA Client users who can have a session on that server at the same time.

Pooling User Counts

Citrix user counts can be shared (pooled) by all servers on the same network subnet. Each server contributes its installed user count to the master ICA Browser.

If server A's user count is 15 and server B's user count is 15, a total of 30 (15+15) is available for use by either server. For example, server A could use up to 20 user counts as long as server B is using no more than 10. You can adjust how many user licenses are allowed to be pooled on a given server. MetaFrame and *WINFRAME* servers use the same user license pool. Citrix servers that pool licenses must be on the same network subnet.

By default, all user counts are pooled.

Note User counts are not pooled across ICA Gateways.

Client Device Licensing

Client device licensing allows users to start multiple sessions on the same or different servers while using only a single Citrix user count. All connections must be from the same client device.

When a user starts a second session on the same Citrix server as the first session, the new session does not consume a second user count.

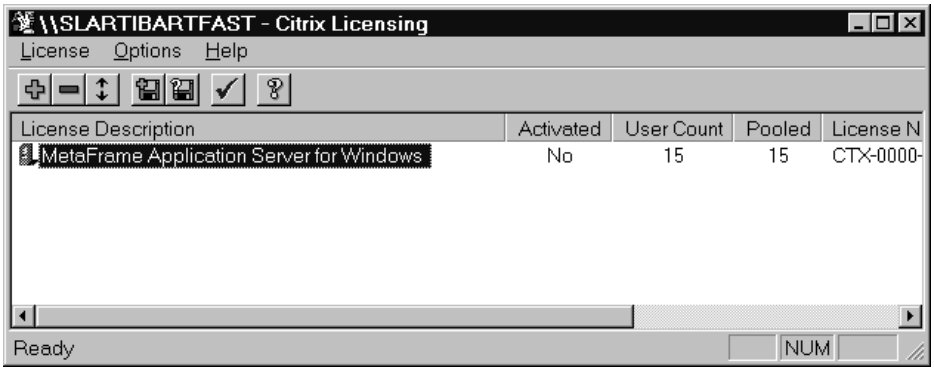
When a user starts a second session on a different Citrix server, the new session does not consume a second user count under the following conditions:

- The first session consumed a pooled user count
- The user makes all connections from the same client device
- All servers are on the same subnet (using the same master ICA Browser)

In addition, if you are using the ICA Win16 or Win32 clients from MetaFrame 1.0 or earlier, all sessions must use the same network protocol (TCP/IP, IPX, NetBIOS).

Important Citrix servers exhaust all local (un-pooled) user counts before giving out pooled user counts. A user assigned a local user count uses a second user count when starting a second session on a different Citrix server.

The Citrix Licensing Program



Use Citrix Licensing to maintain Citrix licenses. With Citrix Licensing, you can:

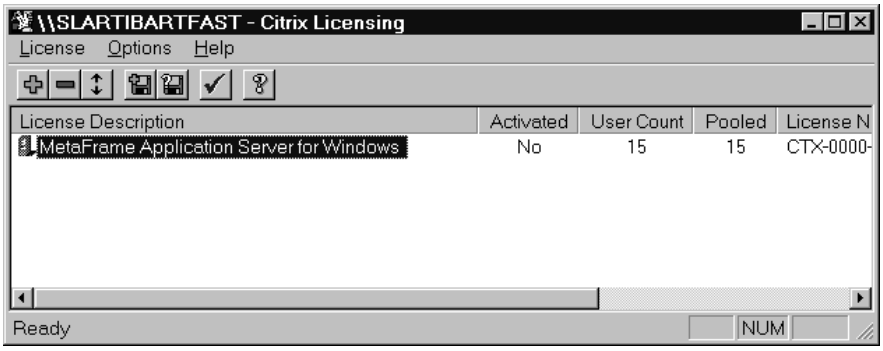
- Add licenses
- Activate licenses
- Adjust the pooled user license count
- Remove licenses
- View a *WINFRAME* license disk
- Print unactivated licenses

Starting Citrix Licensing

▶ **To start Citrix Licensing**

- Click the **Start** button. Point to **Programs**. Point to **MetaFrame Tools**. Click **Citrix Licensing**.

  The Citrix Licensing utility appears, displaying all licenses currently installed on your MetaFrame server.



Each license has an icon to its left that describes the license. The icons are:

Icon	Description
	The license is a base license.
	The license is a server extension license.
	The license is of an unknown type.

Adding a License

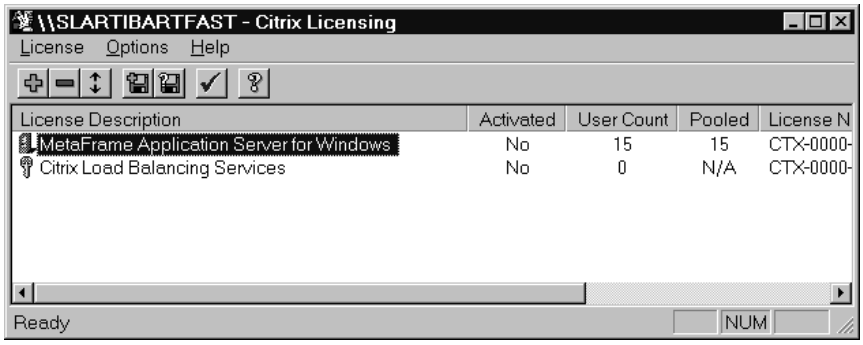
Adding a Citrix license involves three steps:

1. Use Citrix Licensing to add the supplied license serial number.
2. Obtain an activation code for the license.
3. Use Citrix Licensing to enter the activation code for the license.

For more information on activation codes, see “Getting an Activation Code” later in this chapter.

▶ **To add a license serial number**

1. On the **License** menu, click **Add**. The **Enter License Serial Number** dialog box appears.
2. Type the serial number **exactly** as it appears on the serial number sticker on the CD case. Click **OK**. If you enter the serial number incorrectly, an error message appears.
3. A message box containing important information about your license appears, including the grace period before activation is required. Read the information in this box carefully and click **OK** when done.
4. The license number, which is the serial number with an 8-character code appended to make it unique to this server, now appears in the license list:



Disk-Based Licenses

In addition to supporting serial numbers as used with MetaFrame and *WINFRAME* 1.7 or later, MetaFrame also supports the older disk-based licenses used with *WINFRAME* 1.6.

Note When a disk-based license is applied to a MetaFrame server, it is irrevocably converted to a paper-based license. You cannot convert the license back to a disk-based license. You must activate all converted disk-based licenses.

▶ **To add a *WINFRAME* disk-based license**

1. Insert the *WINFRAME* license disk in the disk drive.
2. On the **License** menu, click **Add From Diskette**.
3. Type the letter of the disk drive containing the license disk and click **OK**.
4. A completion message appears. Click **OK**.

Important Once a disk-based license is applied, it cannot be removed and installed again.

5. A message box appears containing important information about the license. Read the information in this box carefully and click **OK** when done.
6. The new license number, with an 8-character code appended, now appears in the license list.

Getting an Activation Code

Citrix uses an activation code-based licensing system. Every licensed Citrix product (Citrix server software or server extension) has an associated serial number. When you install the software, you enter the product's serial number from the product's Serial Number Sticker and get a license number. You must then get an activation code to activate the license.

The activation code is based on the product's license number and is used by the Citrix Licensing program to enable the product. This method offers many benefits, including:

- Your system is usable immediately after you enter your activation code and your software is enabled.
- You can obtain your activation code from the activation server any time.
- You can activate a Citrix server remotely using an administrator account on the Citrix server.
- You have a grace period after you install to activate your software. The grace period for all Citrix licenses is displayed when you install the license. We recommend that you use the grace period to thoroughly test your hardware and software configuration. After you are sure your system is set up properly, you can permanently activate your Citrix software.

See the CD liner notes for information on getting an activation code.

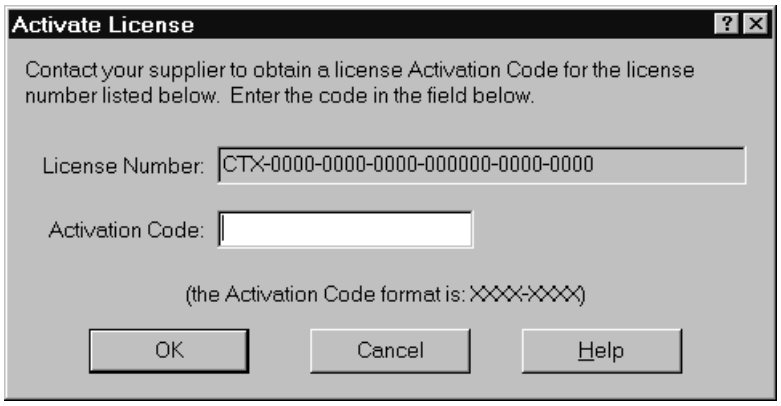
Activating a License

Once a Citrix license is applied, it must be activated.

▶ **To activate a license**

1. Obtain an activation code for the license. For information on getting an activation code, see "Getting An Activation Code" in this chapter.
2. Select the license to activate.

3. On the **License** menu, select **Activate License**. The **Activate License** dialog box appears:



4. Enter your activation code and click **OK**.

Printing Unactivated Licenses

You can print the license number of unactivated licenses. This is useful for archival purposes or to help with license activation.

▶ **To print unactivated licenses**

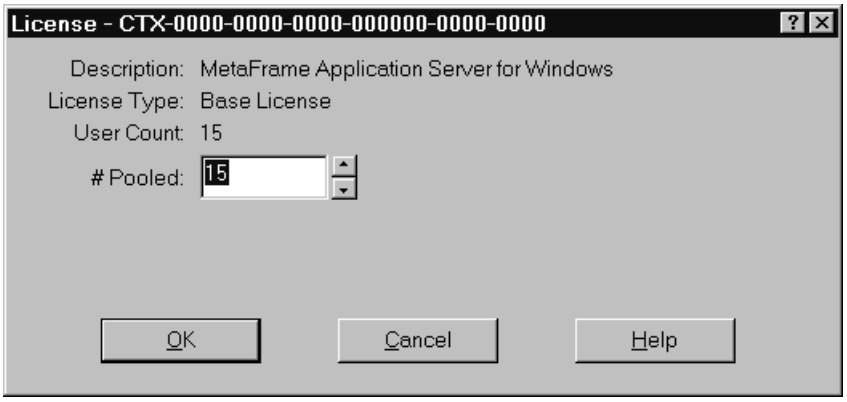
- From the **License** menu, select **Print non-activated Licenses**.

Adjusting the Pooled User Count

By default, all user licenses are pooled. Lowering the number pooled keeps licenses on the local Citrix server. Non-pooled licenses are not available to other Citrix servers and cannot be used for client device licensing.

▶ **To change the number of user counts pooled across Citrix servers**

1. Select the license to adjust.
2. From the **License** menu, click **Change Pool Count**. The **License** dialog box appears:



3. Adjust the pooled user license count for this license.

Removing a License

▶ **To remove a Citrix license**

1. Select the license to be removed. Be sure to write down the complete license number before proceeding.
2. From the **License** menu, click **Remove**.

   The license list now no longer contains the license.

Viewing a *WINFRAME* License Disk

▶ **To view a *WINFRAME* license disk**

1. Insert the *WINFRAME* license disk in the disk drive.
2. From the **License** menu, select **Query Diskette**.
3. Type the letter of the disk drive containing the license disk and click **OK**.

   The **License Diskette** dialog box appears, displaying information about the disk-based license.
4. Click **Close** to exit.

CHAPTER 4

Configuring MetaFrame

Overview

This chapter describes the Citrix MetaFrame extensions to Windows Terminal Server that allow for configuration and administration of the enhanced ICA features. Topics in this chapter include:

- The MetaFrame Administrative Tools
- Managing ICA Connections
- Managing and Monitoring MetaFrame
- Home Directories and Profile Paths

MetaFrame Administrative Tools

This section explains the MetaFrame tools used for administration and the extensions to Terminal Server utilities added by MetaFrame Setup.

▶ **To start MetaFrame tools from the Start menu**

1. Click **Start,** point to **Programs**, point to **MetaFrame Tools**.
2. Click the name of the tool.

You can also use the ICA Administrator Toolbar to quickly access common MetaFrame tools. You can configure the toolbar by right-clicking the toolbar.

Citrix License Activation Wizard

Use the Citrix License Activation Wizard to get activation codes for Citrix Licensing.

For more information on activation codes and using the Activation Wizard, see the CD liner notes and Chapter 3, "Citrix Licensing."

Citrix Connection Configuration

Citrix Connection Configuration is an enhanced version of the Terminal Server Connection Configuration tool. The Citrix Connection Configuration utility adds support for more connections and advanced configurations.

Use Citrix Connection Configuration to:

- Add network, asynchronous, and other types of connections
- Configure existing connections
- Set parameters for mapping client devices
- Set modem parameters
- Test modem configuration

For more information on ICA connections, see "Managing ICA Connections," later in this chapter.

Citrix Licensing

Use Citrix Licensing to:

- Add and remove Citrix base and server extension licenses
- Activate installed licenses
- Pool user licenses across servers
- Restrict user licenses to a single server

For more information on using the Citrix Licensing utility, see Chapter 3, "Citrix Licensing."

Citrix Server Administration

Citrix Server Administration is an enhanced version of the Terminal Server Administration tool.

Use Citrix Server Administration to monitor sessions, users, processes, and published applications on multiple Citrix servers. You can:

- View information about all Citrix servers, Terminal Servers, published applications, domains, and users
- Log users off, disconnect users, and reconnect sessions on the same server or on another Citrix server
- Shadow user sessions on the same server or on another Citrix server
- Reset connections and terminate processes on the same server or on another Citrix server
- Send messages to users on the same server or on another Citrix server
- Configure ICA Browsers and ICA Getaways

For more information on Citrix Server Administration, see "Managing and Monitoring MetaFrame," later in this chapter.

ICA Client Creator

Use ICA Client Creator to create disks you can use to install the Citrix ICA Client and the ICA File Editor on a wide range of client devices.

For more information on using the ICA Client Creator, see the *Citrix ICA Client Administrator's Guides* for the clients you plan to deploy.

ICA Client Printer Configuration

Your end-users can use ICA Client Printer Configuration to:

- Create and connect to ICA Client printers.
- Create print queues for ICA Clients that do not support native print queues, such as the ICA DOS Client.

For more information on using ICA Client Printer Configuration, see the *ICA Client Administrator's Guides* for the clients you plan to deploy.

ICA Client Update Configuration

With Client Auto Update you can store new versions of Citrix ICA Clients in a central c*lient update database.* The latest versions of the ICA Clients are automatically downloaded to ICA Client devices when users connect to the MetaFrame server.

Use ICA Client Update Configuration to manage the client update database.

You can:

- Add or remove Citrix ICA Clients from the update database
- Configure client update options
- Create a new client update database
- Configure the Citrix server to use a default client update database
- Configure client update database options

For more information on updating ICA Clients, see the *Citrix ICA Client Administrator's Guides* for the clients you plan to deploy.

Load Balancing Administration

With Citrix Load Balancing Services, you can load balance published applications installed on multiple servers in a server farm. Load balancing selects a server to run the application or desktop session based on server load.

Use the Load Balancing Administration utility to tune load balancing parameters.

For more information on MetaFrame load balancing, see Chapter 5, "Publishing Applications," and Chapter 6, "Advanced Topics."

Published Application Manager

Use Published Application Manager to configure and manage server farms and published applications. You can:

- Publish applications, videos, and server desktops
- Create template HTML and ICA files for ICA Web Clients
- Create a farm of Citrix servers
- Add a server to a farm
- Change the farm to which a server belongs

For more information on using Published Application Manager see Chapter 5, “Publishing Applications.”

Shadow Taskbar

Use the Shadow Taskbar to shadow multiple users and to quickly switch between shadowed sessions. For more information on using the Shadow Taskbar, see its online help.

Managing ICA Connections

ICA connections are the logical “ports” used by ICA Clients to connect and start a session that runs on the MetaFrame server. A connection is associated with a network connection (IPX, SPX, TCP/IP, or NetBIOS) or a serial connection (modems or direct cables).

The behavior of a user’s session is controlled by settings in three places:

- The ICA Client
- The connection used to start the session
- The user’s account properties

Per-connection settings affect all users that log on at a particular connection. *Per-user settings* affect a single user or group no matter how users connect to the Citrix server. *Per-client* settings can enable additional security and/or compression for remote users.

This section tells you how to configure session behavior for all connections of a given type or all connections on a given asynchronous “port,” that is, how to modify per-connection settings.

For more information on configuring per-user settings, see the User Manager for Domains online help. For more information on configuring per-client settings, see the *Citrix ICA Client Administrator's Guides* for the clients you plan to deploy.

Important The per-connection settings specified in Citrix Connection Configuration take precedence over per-user or per-client settings. If the **inherit user config** check box is selected for a particular setting, the per-user setting overrides the connection setting.

Configuring Connections

Use Citrix Connection Configuration to configure ICA and other connections. This section explains the extensions to Citrix Connection Configuration specific to Citrix MetaFrame. For general connection configuration information, see the Citrix Connection Configuration online help.

During MetaFrame setup, an unlimited number of ICA connections are created for each network type you configure (IPX, SPX, TCP/IP, or NetBIOS), and one asynchronous connection for each configured modem.

Enhancements for supporting ICA connections include adding and configuring asynchronous connections, adding and configuring additional network connections supported by MetaFrame, and configuring Client Device Mapping settings.

All Terminal Server connection options apply to ICA connections.

Adding New ICA Connections

If additional network transports or modems are installed, new connections can be created to provide Citrix ICA Clients access to the MetaFrame server.

The following transports are supported for providing access to the MetaFrame server:

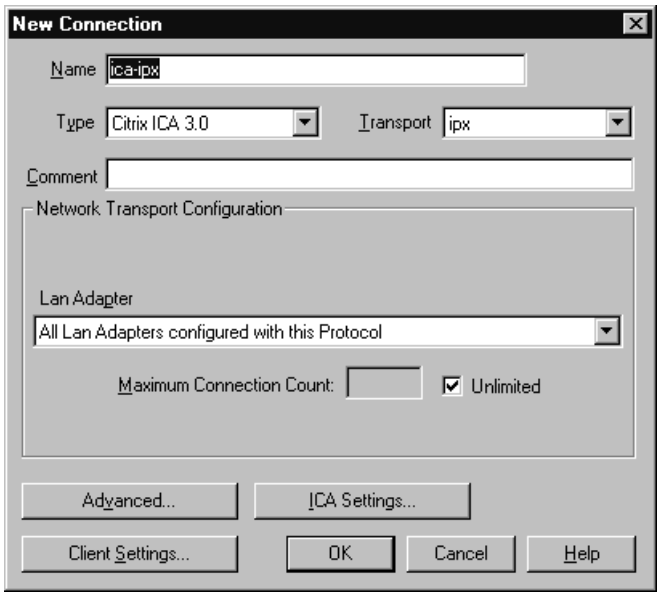
- TCP/IP
- IPX
- SPX
- NetBIOS
- Asynchronous (modem or serial null modem cable connections)

Adding ICA Network Connections

Use the following procedure to add Network ICA connections; for example, if you install an additional protocol such as IPX.

▶ **To create a network ICA connection**

1. Run Citrix Connection Configuration.
2. On the **Connection** menu, click **New**. The **New Connection** dialog box appears:



3. Enter a name for this connection in the **Name** box.
4. In the **Type** list, click **Citrix ICA 3.0**.
5. In the **Transport** list, click the transport protocol.
6. If desired, enter a comment in the **Comment** box.
7. Click **OK**.

Adding ICA Asynchronous Connections

Asynchronous connection types allow direct dial-in to the MetaFrame server without the overhead of RAS and TCP/IP.

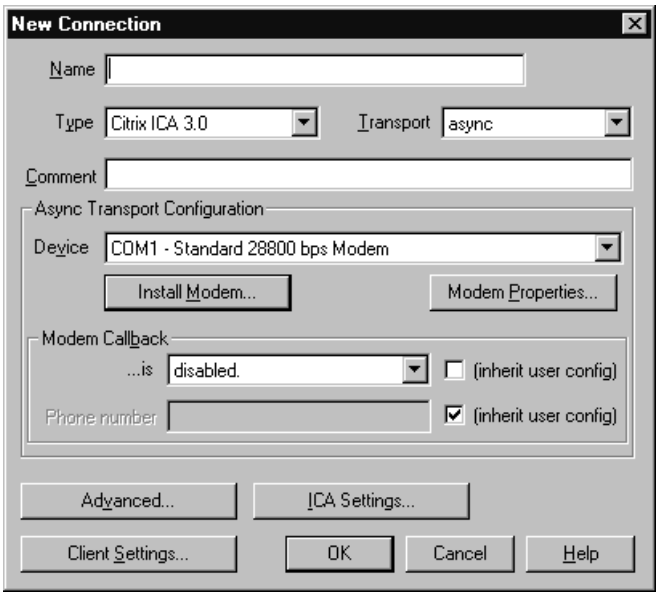
Citrix recommends using high-speed serial port hardware or intelligent multi-port adapters for asynchronous connections. High-speed serial ports and intelligent serial adapters are less CPU intensive, freeing CPU resources that can be devoted to running user sessions.

Note You cannot configure a modem or serial port as both a RAS service port and a connection port.

You cannot configure a serial null modem cable connection using the **Dial-Up Networking Serial Cable between 2 PCs** option. You must configure the connection directly from Citrix Connection Configuration.

▶ **To create an asynchronous ICA connection**

1. Run Citrix Connection Configuration.
2. On the **Connection** menu, click **New**. The **New Connection** dialog box appears.
3. Enter a name for the new connection and click **Citrix ICA 3.0** in the **Type** list.
4. In the **Transport** list, click **async**. The **New Connection** dialog box shows the configuration options for an asynchronous connection:



5. In the **Device** list, click the modem or COM port for this connection. To install a modem, click **Install Modem**. The **Install New Modem** wizard guides you through the process of installing and configuring a new modem.
6. Click **OK**.

Configuring Basic ICA Connection Options

This section provides information on configuration options specific to ICA connections. For information on other connection options, see the Citrix Connection Configuration online help.

ICA network, asynchronous modem, and asynchronous serial null modem cable connections each have different configuration options available. You can modify the configuration of a new network or asynchronous connection in the **New Connection** dialog box. To modify the configuration of an existing connection, double-click the connection in the Citrix Connection Configuration window.

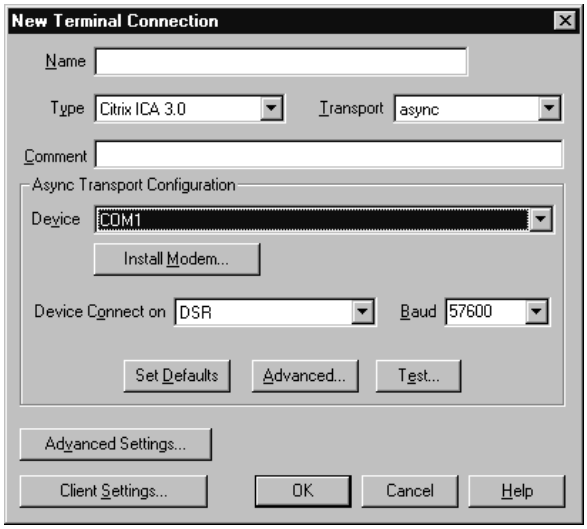
Configuring Modem Callback

You can configure asynchronous ICA connections to hang up and dial a preset or user-specified number after a user logs on to the MetaFrame server. Modem callback options are specified in the **Async Transport Configuration** of an asynchronous connection or in User Manager for Domains if the **inherit user configuration** check box is selected.

If **Modem Callback** is set **to a fixed phone number**, the specified telephone number is always used. If the **inherit user config** check box is selected for **Phone number**, the number specified in the **User Configuration** dialog box in User Manager for Domains is used. You can use a fixed phone number and specify the home phone number of each user to ensure that any Dial-In connections are originating from the user's location.

If **Modem Callback** is set **to a roving phone number**, the user is prompted to enter a callback number when he or she starts an async session. The number specified in the **User Configuration** dialog box in User Manager or Citrix Connection Configuration is used as the default. You can configure callback to a roving phone number to centralize telephone charges.

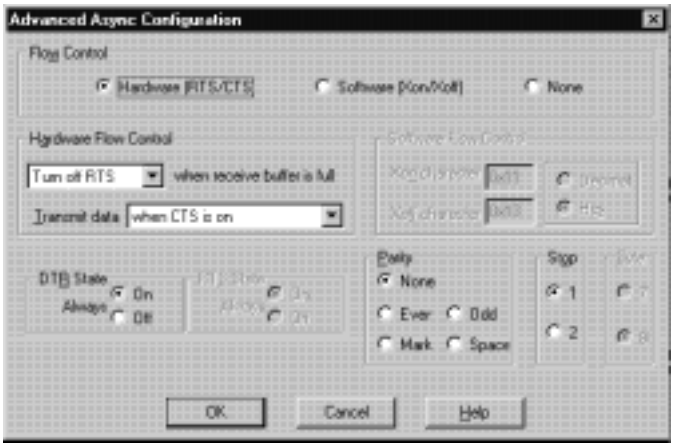
Configuring Async Serial Connections



The **Device Connect On**, **Baud**, **Set Defaults**, **Advanced**, and **Test** options are only present for direct (null modem cable) serial connections. The options for **Async Transport Configuration** include:

Option	Description
Device	The serial port associated with the connection.
Device Connect on	Specifies the signal used to determine when the connection is established and ready for user logon. Options include **CTS**, **DSR**, **RI**, **DCD**, **First Character**, and **Always Connected**.
Baud	Specifies the baud rate.
Set Defaults	Resets the device settings to their default values.
Advanced	Use the **Advanced Async Configuration** dialog box to configure serial port options. See "Configuring Advanced Async Options" below for more information.
Test	Use the **Async Test** dialog box to test the serial port. You can monitor the state of control signals, and transmit data to and receive data from connected devices such as modems. See "Testing Async Connections" below for more information.

Configuring Advanced Async Options



Click **Advanced** in **Async Transport Configuration** to access the **Advanced Async Configuration** dialog box. Use this dialog box to configure the following options:

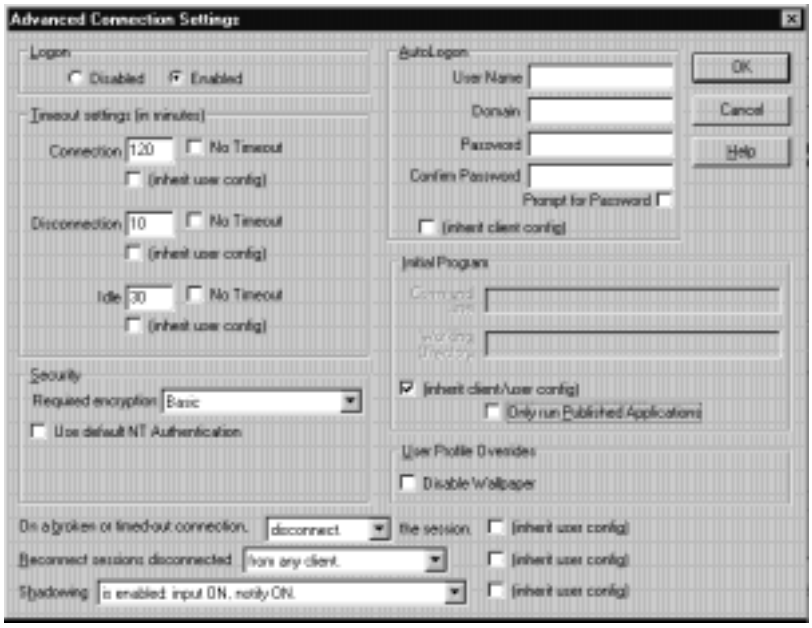
Option	Description
Flow Control	Specifies the type of flow control to use for the connection.
Hardware Flow Control	Specifies the hardware signals that indicate the receive buffer is full.
Software Flow Control	Specifies the characters that stop and start data transmission.
DTR State	Specifies the state of the DTR signal (Always On or Always Off).
RTS State	Specifies the state of the RTS signal (Always On or Always Off).
Parity	Specifies the parity type.
Stop	Specifies the number of stop bits per character.
Byte	The number of data bits per character. Citrix ICA 3.0 requires 8 bits.

Testing Async Connections

Click **Test** in **Async Transport Configuration** to access the **Async Test** dialog box. Use this dialog box to test a serial port and any connected devices.

The name of the serial port and the configured baud rate are displayed at the top of the window, along with a row of modem signal status indicators that show the status of the DTR, RTS, CTS, DSR, DCD, and RI signals. The terminal window allows you to send ASCII data to an attached device and displays any responses from the device. Characters entered are not echoed unless the attached device echoes them.

Configuring Advanced ICA Connection Options



The options on the **Advanced Connection Settings** dialog box in Citrix Connection Configuration provide additional control over security and performance on ICA connections.

The **Advanced Connection Settings** options for Terminal Server connections apply to Citrix ICA connections. For more information about advanced options, see the Citrix Connection Configuration online help.

Restricting Connections to Published Applications

For high-security environments, select the **Only run published applications** check box to restrict the connection to run only published applications defined by the administrator. See Chapter 5, "Publishing Applications," for more information.

Note You cannot specify a published application as the initial program.

Configuring ICA Encryption

You can specify the minimum level of encryption for the ICA connection. The default level is Basic. Strong encryption using the RC5 algorithm is available with Citrix SecureICA Services. SecureICA Services enables RSA RC5 encryption with 40-, 56-, or 128-bit minimum session keys. If the Citrix server is configured to allow RC5 56-bit connections, the Citrix ICA Client can connect with RC5 56- or 128-bit encryption.

Note RC5 56- and 128-bit encryption levels are only available in the United States. Only Basic encryption is available without SecureICA Services installed.

Configuring Session Shadowing

Session shadowing allows you to monitor the display of another active session. Shadowing allows you to see what users are doing and interact with their sessions using the keyboard and mouse. You can shadow active sessions on the same server or on other Citrix servers.

The shadowing settings in the **Advanced Connection Settings** dialog box control the behavior of shadowing for all sessions on the connection.

Option	Description
Enabled	Specifies that sessions on the connection can be shadowed.
Disabled	Specifies that sessions on the connection cannot be shadowed.
Input On	Allows the shadower to input keyboard and mouse actions to the shadowed session.
Notify On	Specifies that the shadowed user gets a message asking if it is OK for the shadowing to occur.

Configuring ICA Settings

Use the **ICA Settings** dialog box for configuring ICA-specific connection settings.

Configuring ICA Audio

Client Audio Mapping can cause excessive load on the Citrix server and network. The higher the audio quality, the more bandwidth is required to transfer the audio data. Higher quality audio also uses more server CPU to process. Three different audio quality settings are available, or client audio mapping can be disabled completely.

Audio quality is set on a per-connection basis, but is also configurable on the client computer. If the client and server audio quality settings are different, the lower of the two settings is used.

The **Client Audio Quality** options are:

- **High**. This setting is only recommended for connections where bandwidth is plentiful and sound quality is important. This setting allows clients to play a sound file at its native data rate. Sounds at the highest quality level require about 1.3Mbps of bandwidth to play clearly. Transmitting this amount of data can result in increased CPU utilization and network congestion.
- **Medium**. This setting is recommended for most LAN-based connections. This setting causes any sounds sent to the client to be compressed to a maximum of 64Kbps. This compression results in a moderate decrease in the quality of the sound played on the client computer. The host CPU utilization can decrease compared with the uncompressed version due to the reduction in the amount of data to be sent across the wire.
- **Low**. This setting is recommended for low-bandwidth connections, including most modem connections. This setting causes any sounds sent to the client to be compressed to a maximum of 16Kbps. This compression results in a significant decrease in the quality of the sound. The CPU requirements and benefits of this setting are similar to those of the Moderate setting; however, the lower data rate allows reasonable performance for a low-bandwidth connection.

Configuring Client Device Mapping

The Citrix ICA Clients support mapping devices on client computers so they are available to the user from within a remote control ICA session. You do not need a network or RAS connection to use ICA client device mapping. Users can:

- Transparently access local drives, printers, and COM ports
- Cut and paste between the ICA session and the local Windows clipboard
- Hear audio (system sounds and .wav files) played from the ICA session

During logon, the ICA Client informs the server of the available client drives, COM ports, and LPT ports. By default, client drives are mapped to server drive letters and server print queues are created for ICA Client printers so they appear to be directly connected to the MetaFrame server.

These mappings are available only for the current user during the current session. They are deleted when the user logs off and recreated the next time the user logs on.

The MetaFrame server lists all client disk and printer devices under the **Client Network** icon in **Network Neighborhood**.

During a session, users can use ICA Printer Configuration to map client devices not automatically mapped at logon. For more information on using the ICA Printer Configuration utility, see the *Citrix ICA Client Administrator's Guides* for the clients you plan to deploy.

Controlling Client Device Mappings

Client device mapping options are specified in the **Client Settings** dialog box in Citrix Connection Configuration.

The **Connection** options control whether drives and printers are mapped to client drives and printers. If these options are cleared, the devices are still available but must be mapped to drive letters and port names manually.

Option	Description
Connect client drives at Logon	If this option is checked, the client computer's drives are automatically mapped at logon.
Connect client printers at Logon	If this option is checked, the client computer's printers are automatically mapped at logon. This only applies to Windows clients and only maps printers already configured in Print Manager on the client computer. DOS printers must be manually mapped.
Default to main client printer	If this option is checked, the user's default client printer is configured as the default printer for the ICA session.
(inherit user config)	If this option is checked, the per-user settings in User Manager are used.

To automatically connect to only the printer configured as the default printer when the user logs on, select the **By default, connect only the client's main printer** check box.

Default printers can be set on the ICA Client device. Users can override the default printer mapping with ICA Client Printer Configuration. For more information on ICA Client Printer Configuration, see the *Citrix ICA Client Administrator's Guides* for the clients you plan to deploy.

Use the **Client Mapping Overrides** to disable client device connections.

Client Drive Mapping

Client drive mapping is transparently built into the standard Citrix device redirection facilities. The client drives appear as a network type (Client Network) in Network Neighborhood. The client's disk drives are displayed as shared folders with mapped drive letters. These drives can be used by Windows Explorer and other applications like any other network drive.

How MetaFrame Assigns Drive Letters to Mapped Client Drives

By default, the drives on the client system are automatically mapped to drive letters on the MetaFrame server during logon. The server tries to match the client drives to the client drive letters; for example, the client's first floppy disk drive to A, the second floppy disk drive to B, the first hard drive partition to C, etc. This allows the user access to client drive letters in the same way from local or remote sessions.

These drive letters are often used by the drives on the MetaFrame server. In this case, client drives are mapped to other drive letters. The MetaFrame server starts at V and searches backward for free drive letters.

See Chapter 2, "Installing MetaFrame," for information on changing server drive letters during MetaFrame Setup.

Reassigning Server Drives

The MetaFrame server tries to match the client drives to the client drive letters; for example, the client's first floppy disk drive to A, the second floppy disk drive to B, the first hard drive partition to C, etc. MetaFrame Setup offers to move the Terminal Server drives to allow ICA Client drives to map to their local drive letters.

If you want to change the server drive letter assignments after MetaFrame Setup is complete, you should change the drive letters before installing any applications. If you have already installed applications, their INI files and registry settings may point to the wrong drive letters and cause the applications to operate incorrectly.

▶ **To change drive letter assignments**

1. No users should be logged into the system and all programs must be closed. Logon as an administrator at the MetaFrame server console.
2. Start Disk Administrator.
3. Select the first drive partition, usually C. On the **Tools** menu, click **Assign Drive Letter**.

   Enter the drive letter for the first partition. Most ICA client computers have one or two hard drives. Therefore, setting the MetaFrame server drives starting at drive M or N should leave enough drive letters free for client drives. Click **OK** to make the change. If you change the partition containing the %systemroot% directory, an error message appears stating that the drive is being used. Click **OK**. Disk Administrator offers to set the drive to change and reboot the server when you exit Disk Administrator.

4. Repeat Step 3 for each subsequent partition. Assign drive letters sequentially in the same order they were originally assigned. If a CD-ROM drive is present, it should be sequentially last in the drive letter list.
5. On the **Partition** menu, click **Commit Changes Now**. This saves the changes and reboots the system.

When the system reboots, the drive letters are changed to the new drive letters. You can install applications, set up users, and configure connections. When ICA Clients log on to the MetaFrame server, their drives map to the local client drive letters. Users can access and use their local drives as they normally would.

Controlling Drive Mapping Assignments When Using NetWare Login Scripts

Client drive mapping and NetWare login script execution occur in parallel. If the login script maps NetWare network drives, it is possible that a user could find drive V mapped to his client drive C during one session but mapped to a NetWare drive during another.

This problem can be avoided by adding two registry values in **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix**:

REG_SZ: InitialClientDrive
Defines the first drive letter to use for client drive mapping. The system searches backward through the alphabet to assign drive letters to client drives that could not be mapped to their "native" drive letters.

REG_SZ: InitialNetWareDrive
Defines the drive letter to use for the NetWare SYS:LOGIN directory that is mapped to the preferred server during the initial NetWare attachment. This setting is the equivalent of the DOS VLM Net.cfg setting "First Network Drive." If this value is not set, the first available drive letter starting with C and working up to Z is used for this mapping.

Client Printer Mapping

Client printer mapping allows a remote application running on the Citrix server to access printers attached to the client computer. The client mappings appear as another network type (Client Network) to Print Manager.

ICA Client printers are automatically mapped when a user logs on and automatically deleted when the user logs off if they do not contain any print jobs. If print jobs are present, the printer (and its associated jobs) is retained.

For information on mapping client printers, see the *Citrix ICA Client Administrator's Guides* for the clients you plan to deploy.

Client COM Port Mapping

Client COM port mapping allows a remote application running on the Citrix server to access devices attached to COM ports on the client computer. Client COM ports are not automatically mapped to server ports at logon, but can be mapped manually using the **net use** or **change client** commands. See Appendix A, "MetaFrame Command Reference," for more information on the **change client** command.

For more information on client COM port mapping, see the *Citrix ICA Client Administrator's Guides* for the clients you plan to deploy.

Client Audio Mapping

Client audio mapping allows applications running on the Citrix server to play sounds through a Sound Blaster Pro-compatible sound device on the client computer. The MetaFrame server can control the amount of bandwidth used by client audio mapping. Audio mapping is configured per-client and per-connection in the **ICA Settings** dialog box.

For more information on using client audio mapping, see the *Citrix ICA Client Administrator's Guides* for the clients you plan to deploy.

Managing and Monitoring MetaFrame

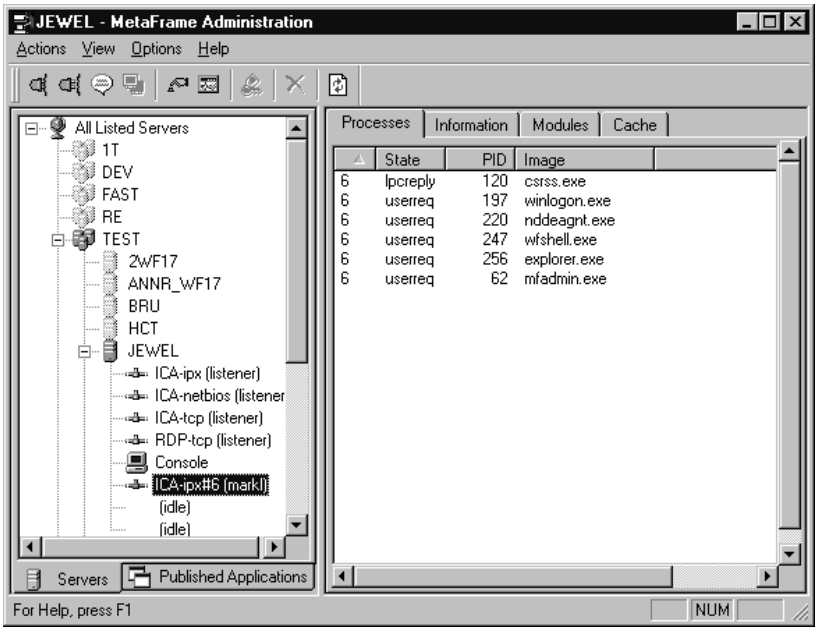
Citrix Server Administration is an enhanced version of the Terminal Server Administration tool. Citrix Server Administration provides cross-server functionality, allowing you to monitor an entire enterprise from a single location.

Use Citrix Server Administration to monitor sessions, users, processes, and published applications on multiple servers. You can:

- View information about servers, published applications, domains, and users
- Log users off, disconnect users, and reconnect sessions
- Shadow user sessions on the same server or on another Citrix server
- Reset connections and terminate processes
- Send messages to users
- Configure ICA Browsers and ICA Getaways

The Citrix Server Administration Window

The Citrix Server Administration window has two panes. The left pane displays Citrix servers, domains, Terminal Servers, sessions, and published applications. The right pane has several tabs that you can use to display information about the objects selected in the left pane.



The tabs displayed in the right pane change depending on the type of selected object; for example, if a session or server is selected. If you select a Citrix server in the left pane of the Citrix Server Administration window, the **Users**, **Sessions**, **Processes**, **Licenses**, **ICA Browser**, and **Information** tabs are displayed in the right pane of the Citrix Server Administration window. If you select an active session in the left pane of the Citrix Server Administration window, only the **Processes**, **Cache**, **Modules**, and **Information** tabs are displayed in the right pane of the Citrix Server Administration window. If you select an idle connection, no information is displayed.

Viewing Server Information

When Citrix Server Administration is started, your current MetaFrame server is the selected object. Other MetaFrame servers and other domains on the network appear with a gray icon. By default, Citrix Server Administration gathers information only from your server. To connect to other servers and view information about them, click the server name or double-click the domain in the left pane.

Click the **Published Applications** tab to switch the left pane to the published applications view. This view shows the published applications on the network.

Click the **Video Servers** tab to switch the left pane to the video servers view. This view shows Citrix video servers on the network.

Click the **Servers** tab to return to the servers view.

To display all the domains, servers, and sessions in the left pane of the Citrix Server Administration window, click **Expand All** on the **View** menu.

Citrix Server Administration Views

The right pane of the Citrix Server Administration window has several tabs that you can use to display information about the objects selected in the left pane.

The tabs that are displayed in the right pane change depending on the type of selected object; for example, if a session or published application is selected.

For detailed descriptions of the information and settings for each tab, see the Citrix Server Administration online help.

Connecting to Servers

By default, Citrix Server Administration connects only to the server from which it is running. To connect to a new server and gather information on that server, click the servername in the left pane. You can connect to all servers by clicking **All Listed Servers** and clicking **Connect to All Servers** on the **Action** menu. Click **Connect to All Servers in Domain** on the **Action** menu to contact all servers in the domain. This option is available only when a domain is selected in the left pane.

Note The list of servers in a domain may shrink after connecting to all servers. Citrix Server Administration displays information only about Citrix servers and Terminal Server systems. Other servers are removed from the domain list.

Servers Tab

The **Servers** tab is available when a domain, published application, or **All Listed Servers** is selected in the left pane. The **Servers** tab displays information about all servers Citrix Server Administration is currently monitoring. By default, Citrix Server Administration connects only to the server from which it is running. The fields shown are different for domains, **All Listed Servers**, and published applications.

Applications Tab

The **Applications** tab is available when **Published Applications** is selected in the published applications pane. The **Applications** tab displays information about applications published on the network.

Users Tab

The **Users** tab shows information about currently logged on users. Clicking a server in the left pane shows all users with sessions on that server. Clicking a domain shows users with sessions on all servers. Clicking on a published application shows all users connected to the application.

Sessions Tab

The **Sessions** tab shows the status of all sessions. Clicking a server in the left pane shows all sessions on that server. Clicking a domain shows sessions on all servers in the domain. Click **All Listed Servers** to view sessions on all servers.

Processes Tab

The **Processes** tab displays the status of all user (and optionally all system) processes associated with the selected object (session, server, domain, or **All Listed Servers**), one process per line.

Licenses Tab

The **Licenses** tab displays information about the Citrix software licenses on the selected server, domain, or **All Listed Servers**. When a server or **All Listed Servers** is selected in the left pane, information on current license use is displayed.

ICA Browser Tab

The **ICA Browser** tab displays ICA Browser settings and allows you to configure the ICA Browser service on the selected server. See “Configuring the ICA Browser,” later in the chapter for more information.

Information Tab

The **Information** tab displays information about the selected server, session, or published application. The fields shown are different for each object selected in the left pane.

Server

When a server is selected in the left pane, information on the software and build number is displayed.

Session

When a session is selected in the left pane, information on the user, session, and client is displayed.

Published Application

When a published application is selected in the left pane, information on the published application is displayed.

Modules Tab

The **Modules** tab displays the files in use by the Citrix ICA Client when a session is selected. The **Modules** tab can be used to diagnose problems with the connection. The information is available only for Citrix ICA Clients.

Cache Tab

The **Cache** tab displays information on the Citrix ICA Client cache state when a session is selected in the left pane. The **Cache** tab is available only for Citrix ICA Clients.

ICA Gateways Tab

The **ICA Gateways** tab displays configured ICA Gateways. You can use the **ICA Gateways** tab to add and remove ICA Gateways. An ICA Gateway is used to allow ICA Clients or servers to contact Citrix servers on a different network subnet.

Streams Tab

The **Streams** tab displays the current status of all video streams.

Settings Tab

The **Settings** tab displays VideoFrame settings. You can configure the VideoFrame server settings for the selected server. For more information on VideoFrame settings, see the *VideoFrame Administrator's Guide* included with Citrix VideoFrame.

Managing Servers, Users, Sessions, and Processes

Use the Citrix Server Administration utility to manage the users, sessions, and processes on a Citrix server or Terminal Server. You can connect and disconnect sessions, shadow ICA sessions, reset sessions in case of error, manage processes, and send messages to users on your server or on other servers on the network.

Disconnecting a Session

To disconnect a session, click **Disconnect** on the **Action** menu. Disconnecting a session closes the connection between the server and client; however, the user is not logged off and all running programs remain.

If the user logs on to the server, the disconnected session is reconnected to the client.

Connecting to a Disconnected Session

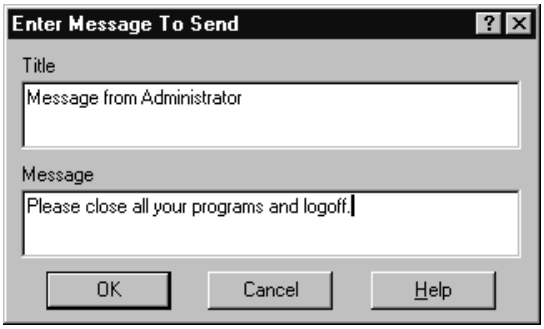
A disconnected session shows **disc** in the **State** field. You can connect to a disconnected session by clicking the session and clicking **Connect** on the **Action** menu. Your current session is disconnected and the selected session is connected to your session.

Note Your session must be capable of supporting the video resolution used by the disconnected session. If the session does not support the required video resolution, the operation fails. Sessions disconnected from connections other than the console cannot be connected to the system console.

Sending Messages to Users

You can send a message to users informing them of problems or asking them to log off the server.

To send a message, click an active user and click **Send Message** on the **Action** menu. If you select multiple users, the message is sent to each user.



In **Title**, enter the text for the title of the message dialog box. In **Message**, enter the text of the message. Click **OK** to send the message. The message appears on the user's screen:

Note Multiple lines can be entered in either box by using CTRL+ENTER to move to a new line in the edit box.

Shadowing a User's Session

You can monitor the actions of users by shadowing their sessions. The shadowed session is displayed in the shadower's session. The shadowed session can be controlled by the mouse and keyboard of the shadowing session. By default, the user being shadowed is asked to allow or deny session shadowing. Keyboards, mouse, and notification options can be controlled from the Citrix Connection Configuration utility for connections, or from User Manager for Domains for individual users.

To start shadowing a session, click on the session to shadow and click **Shadow** on the **Action** menu.

You can change the hotkey used to terminate shadowing, if desired. The default hotkey to terminate shadowing is CTRL+*.

The user is notified of the pending shadowing and asked to allow or deny shadowing, unless notification is disabled for the user in User Manager for Domains or in Citrix Connection Configuration.

The shadowing session must be capable of supporting the video resolution used by the shadowed session. If the shadowing session does not support the required video resolution, the operation fails.

You cannot shadow the system console from another session. You cannot use Citrix Server Administration to shadow other sessions from the system console. To shadow sessions from the system console, use the Shadow Taskbar.

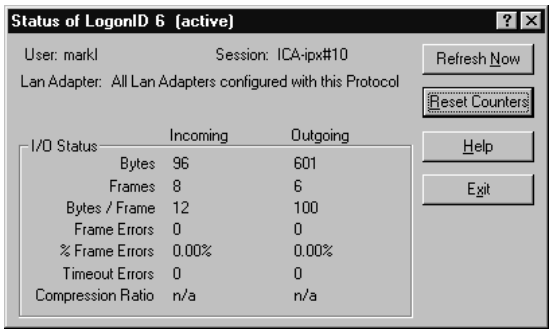
Resetting a Session or Connection

You can reset a session in case of an error. Resetting the session terminates all processes running on that session. Resetting a session may cause applications to close without saving data.

If you reset the special **Listen** session, all sessions for that connection are reset.

Displaying Connection Statistics for a Session

To monitor the status of a session, select the session and click **Status** on the **Action** menu.



The **Status of…** dialog box displays information about the session and connection statistics.

By default, Citrix Server Administration updates **I/O Status** information every second. You can change the refresh rate by clicking **Preferences** on the **Options** menu. If **Status Dialogs Refresh** in the **Preferences** dialog box is set to **Refresh Manually**, you can refresh to connection statistics by clicking **Refresh Now**.

Click **Reset Counters** to zero the **I/O Status** counters.

Logging Users off the Server

You can forcefully end a user's session by selecting the user in the **Users** tab and clicking **Logoff** on the **Action** menu. If you select multiple users, each user is logged off.

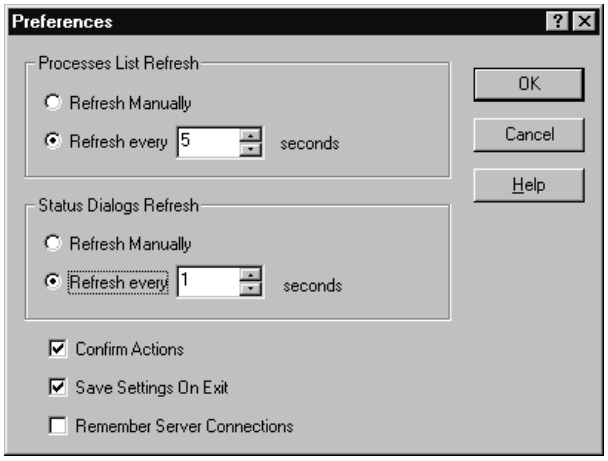
Logging off users without giving them a chance to close their applications can result in data loss.

Terminating Processes

You can forcefully end a user or system process by selecting the process from the **Process** tab and clicking **Terminate** on the **Action** menu. Terminating a user process can result in the loss of data. Terminating a system process can cause the server to become unstable.

Preferences for Citrix Server Administration

Use the **Preferences** dialog box to configure the Citrix Server Administration utility. Click **Preference** on the **Options** menu to display the **Preferences** dialog box.



In **Process List Refresh**, select **Refresh Manually** to update the **Process** tab list manually. Select **Refresh every *x* seconds** and enter the number of seconds to refresh the process list automatically.

In **Status Dialogs Refresh**, select **Refresh Manually** to update the **I/O Status** counters manually. Select **Refresh every *x* seconds** and enter the number of seconds to refresh the counters automatically.

Select the **Confirm Actions** check box to turn on confirmation messages before performing destructive actions.

Select the **Save Settings on Exit** check box to save your current settings when Citrix Server Administration closes.

At startup, Citrix Server Administration connects only to the server from which it is running. If you want Citrix Server Administration to reconnect to all the servers you were connected to previously, select the **Remember Server Connections** check box.

Configuring the ICA Browser

The ICA Browser maintains data on Citrix servers and published applications. You can configure the ICA Browser by selecting a server and clicking the **ICA Browser** tab.

Settings on this tab affect the operation of the ICA Browser service. The default settings work for most installations and should be changed only when you understand the implication of each setting.

For more information on the ICA Browser tab settings, see the Citrix Server Administration online help. For more information on the ICA Browser service, see "Understanding the ICA Browser Service," later in this chapter.

Connecting Citrix Servers Across Network Subnets

Use ICA Gateways to allow ICA Clients or servers to contact Citrix servers on a different network subnet. You can configure the ICA Gateways for a network by clicking **All Listed Servers** in the **Server** view and clicking the **ICA Gateways** tab.

For information on configuring ICA Gateways with Citrix Server Administration, see the Citrix Server Administration online help. For information on ICA Gateways, see "Understanding ICA Gateways," later in this chapter.

Configuring VideoFrame Servers

You can configure a VideoFrame server in the **Video Servers** pane. Select a video server and click the **Settings** tab.

For more information on VideoFrame settings, see the *VideoFrame Administrator's Guide* included with Citrix VideoFrame.

Controlling New Logons

You can prevent new logons to a Citrix server by selecting the server in the **Server** pane, right-clicking on the server, and clicking **Disable New Logons**.

You can disable new logons to install new software or to do other system maintenance.

Understanding the ICA Browser Service

The ICA Browser maintains data on Citrix servers and published applications. Separate data is maintained for each network transport (TCP/IP, IPX, and NetBIOS). The ICA Browser consists of a master browser, member browsers, and client systems. The ICA Browser uses directed packets to communicate with other ICA Browser services running on Citrix servers.

The ICA Browser service maintains a list of available Citrix servers and published applications for a given network and transport type.

Citrix ICA Clients query the ICA Browser service to obtain a list of Citrix servers and published applications. The Citrix ICA Client queries the ICA Browser service for the network address of servers and published applications when a session is launched. Citrix servers use the ICA Browser service to pool licenses and share administrative and performance information.

The ICA Browser Service

Every Citrix server runs the ICA Browser service. One Citrix server is elected the *master browser*; all other Citrix servers on the network are *member browsers*. Each physical network of Citrix servers has one master browser per protocol. The master browser for each network is chosen by a *master browser election.* If the current master browser on a network goes down, a new master browser election is held. This provides high reliability for the ICA Browser service.

The master browser keeps track of the following information:

- The available Citrix servers
- The available published applications
- Any pooled licenses
- Performance and load information for Citrix servers

The Master Browser

The master browser maintains the browse list and periodically obtains updates from the member browsers (Citrix servers) on the same network. Each transport protocol (TCP/IP, IPX, and NetBIOS) has its own master browser.

The master browser is an ICA Browser acting as a central information store. An ICA Browser becomes the master browser after winning a browser election.

Browser Elections

The ICA Browser system elects a master browser under the following conditions:

- The current master browser does not respond to another ICA Browser
- The current master browser does not respond to an ICA client
- A Citrix server is started
- Two master browsers are detected on the same network subnet

A set of election criteria is used to choose a master browser. An ICA Browser starts a browser election by broadcasting its election criteria. If another browser has a higher election criteria, it broadcasts its own election criteria. Otherwise, the last ICA Browser to respond to the election becomes the master browser.

Five criteria, in order, are used to elect a master browser:

1. The version number of the ICA Browser (most recent gets precedents)
2. Configured as the master browser with Citrix Server Administration (or the registry key that specifies master browser status)
3. The Citrix server is also a Windows NT domain controller
4. The length of time the ICA Browser has been running
5. The *computername* of the Citrix server

For example, a Citrix server has been running two hours longer than a second Citrix server. If the second server is running a later version of the ICA Browser service, the second server wins the master browser election.

Warning The master ICA Browser election criteria has changed in this release. The version number of the ICA Browser is the highest criteria and overrides an ICA Browser specifically configured in the registry as the master ICA Browser.

If you have designated a fixed (hard-coded) master ICA Browser in an existing Citrix server farm, install MetaFrame 1.8 on the master ICA Browser machine first. If you install MetaFrame 1.8 on another server first, that server will become the master ICA Browser.

The Citrix Server Administration option that prevents a MetaFrame 1.8 server from becoming the master ICA Browser also disables certain MetaFrame 1.8 features.

How ICA Clients Use the Master ICA Browser

Citrix ICA Clients must locate the master browser to get the address of a server or published application. The Citrix ICA Client can locate the master browser by sending out broadcast packets, or, if the address of a Citrix server is specified in the Citrix ICA Client or in an ICA file, the ICA Client locates the master browser by sending directed packets to the specified address. The ICA Client requests the address of the ICA master browser from the Citrix server.

Locating the Current Master ICA Browser

You can use the **query server** command to discover the Citrix server acting as the master browser. The **query server** command displays all servers on each network transport (TCP/IP, IPX, and NetBIOS). An **M** next to the network address of a server indicates that it is the master browser for that network transport.

Understanding ICA Gateways

In order for Citrix servers or ICA Clients to contact Citrix servers on a different network, an *ICA Gateway* must be used. An ICA Gateway is established between two networks to allow the master browsers on each network to share information about available Citrix servers and published applications.

The ICA Browser service uses directed packets to exchange information. An ICA Gateway is used to connect the ICA Browser services of Citrix servers on different network subnets. ICA Gateways are used on routed networks such as TCP/IP and IPX.

An ICA Gateway consists of at least two Citrix servers. The *local server* is responsible for contacting the other network and setting up a link between the master browsers on each network. The *remote server* is a Citrix server on the other network that communicates with the local server to establish the ICA Gateway. You can store redundant gateway information on different servers to increase reliability by selecting multiple servers.

ICA Gateway Routing

To enable ICA Gateways to work correctly, network routers must pass ICA Browser traffic between subnets.

ICA Gateways on TCP/IP networks use directed UDP datagrams to port 1604. Routers on TCP/IP networks must be configured to route UDP datagrams between network subnets.

For ICA Gateways to function on IPX networks, routers must be configured to route raw IPX packets.

For more information on the ICA Browser service, see “Understanding the ICA Browser Service” earlier in this chapter.

Home Directories and Profile Paths

If you have *WINFRAME* and Terminal Server servers in the same domain, the Terminal Server profile path box references the same data as the *WINFRAME* profile path box. The *WINFRAME* servers ignore the Terminal Server home directory path and use the Home directory path instead.

CHAPTER 5

Publishing Applications

Overview

This chapter describes application publishing. Topics in this chapter include:

- An introduction to application publishing, Program Neighborhood, and server farms
- Configuring Server Farms
- Viewing Servers and Published Applications
- Publishing Applications
- Maintaining Published Applications

Introduction

Published applications:

- Give ICA Client users easy access to applications running on Citrix servers
- Increase your control over application deployment
- Shield users from the mechanics of the Windows NT server environment hosting the ICA session

The Citrix utility Published Application Manager, with its support for server farms and Program Neighborhood, is the main tool for publishing applications.

The following topics describe how to simplify user access to applications running on Citrix servers while increasing your control over deployment.

User Access

When you publish applications, user access to those applications is greatly simplified in three areas:

- **Addressing**. Instead of connecting to a Citrix server by its IP address or server name, ICA Client users can connect to a specific application by whatever name you give it. Connecting to applications by name eliminates the need for users to remember which servers contain which applications.
- **Navigation of the server desktop**. Instead of requiring client users to have knowledge of the Windows NT 4.0 and/or 3.51 desktop (Windows NT Explorer or Program Manager) to find and start applications after connecting to Citrix servers, published applications present the ICA Client user with only the desired application in an ICA session.
- **User authentication**. Instead of logging on and logging off multiple Citrix servers to access applications, Program Neighborhood users can authenticate themselves a single time to all servers and obtain immediate access to all applications configured for their user group or specific user name. Also, publishing applications for the special Citrix *anonymous* user group lets you completely eliminate the need for user authentication for those applications you want to provide to all users on your network.

Program Neighborhood

Program Neighborhood facilitates user access to published applications by eliminating the need for client-side configuration of connections. Program Neighborhood presents application sets to client users. An *application set* is a user's view of the applications published on a given server farm, which that user is authorized to access. Each user performs a single authentication to all servers in a farm and is then presented with an application set containing each application configured for his or her specific user account or user group. Published applications appear as icons in the view of the farm and are pre-configured for such connection properties as session window size and colors and supported level of encryption, audio, and video.

Note Program Neighborhood is the program users run to connect to MetaFrame servers with the Citrix ICA Client for Win32 (Windows 95, Windows 98, and Windows NT platforms).

Using Program Neighborhood greatly simplifies the process of locating and connecting to published applications. For example, if you want your ICA Client users to have access to a word processing program, they can do either of the following:

- Start the ICA Client on the client device; get an IP address or server name of a Citrix server from an administrator or from the server browsing service provided in ICA Clients; start the ICA Client's connection wizard, specify the address and configure connection options such as encryption, window size, and color, double-click the connection object; log on to the Citrix server desktop; navigate the desktop for the word processing program's desktop shortcut, Start menu shortcut, or Program Manager program group. Then, if the user needs access to another application, and the application exists on another Citrix server, the ICA Client user must repeat the process.
- Start Program Neighborhood, perform a single logon that authenticates the user to all published applications in an application set, double-click an icon for the word processing program. Starting additional applications requires simply double-clicking their icons in Program Neighborhood.

Application publishing benefits users of other, non-Program Neighborhood ICA Clients (such as the UNIX, Macintosh, DOS and Web Clients) as well. Although they do not support the complete (server and client-side) administrative configuration of the ICA connection provided by Program Neighborhood, these ICA Clients do support connections to published applications.

In the case of the ICA UNIX, Macintosh, and DOS Clients, client users can benefit from application publishing's simplified addressing and desktop navigation when they configure connections to published applications using their connection configuration managers.

In the case of the Web Client (available as an Internet Explorer Active-X control, Netscape plug-in, or Java applet), you can create Web access that lets users of client devices running a Web browser and an ICA Web Client click a link in a Web page to start a published application.

Tip To give a broader range of your users the benefits of the new Program Neighborhood features, you can publish the ICA Win32 (Program Neighborhood) Client application on your Citrix servers. Users of the non-Win32 Citrix ICA Clients can then define in their connection managers a single connection to the Program Neighborhood published application. Once they connect to the Program Neighborhood published application, they can launch all other applications published on all the Citrix servers in your farm from a single easy interface.

Administrative Control

When you publish applications, you get greater administrative control over application deployment with:

- **Selected user access**. You publish applications for specific users and user groups. By definition, an application you publish for a specific user group is unavailable to other groups.
- **Enabled and disabled application access**. You can temporarily restrict all access to an application by disabling it. You can enable the application later to return access to users. This capability is useful when you want to take an application offline for maintenance.
- **Multiple-server application hosting**. Application publishing, when used in conjunction with Citrix Load Balancing Services, lets you direct ICA Client connection requests to the least busy server in a farm of servers configured to run an application.

Server Farms

Citrix server farms provide you with a flexible and robust way of deploying applications to ICA Client users. Server farms let you centralize your control over the application deployment process by grouping Citrix servers into a single administrative unit. Citrix servers in a farm function together to make applications easily available to your ICA Client users.

A *server farm* is a group of Citrix servers managed as a single entity and that share some form of physical connection and a common base of user accounts. After you place your servers in a server farm, you can publish applications on servers in the farm for users in the common base of accounts. After starting Program Neighborhood, a user logs in once, then sees an application set containing each application configured for his or her specific user account or user group.

Types of Applications You Can Publish

When you publish an application, the server you specify to host the application stores configuration information for the application in its registry. The collection of registry entries governs the properties of the ICA connection including:

- The application to run in the session
- Users who can connect to the application
- In the case of an application published in a server farm, client-side session properties such as window size and colors and supported level of encryption, audio, and video

To the ICA Client user, a published application is an application that appears very similar to an application running locally on the client device. The way the user starts the application depends upon the ICA Client in use on the client device.

Program Neighborhood users	After starting Program Neighborhood, these users find a list of applications published for their user account or user group.
ICA UNIX, Macintosh, and DOS Client users	Using connection managers, these ICA Client users can browse a list of all applications published on the network and select an application to run.
ICA Web Client users	These users can click a link in a Web page.

Published Application Manager supports four types of published applications.

Standard Applications

You can publish any application that can run on the Windows NT console (32-bit Windows applications, 16-bit Windows applications, DOS applications, POSIX applications, and OS/2 applications).

Citrix Installation Management Services Applications

In order to publish Citrix IMS applications, you must install Citrix Installation Management Services on your network. Citrix Installation Management Services performs remote unattended installation of applications on Citrix servers. Using IMS, you can simultaneously install an out-of-the-box application on all Citrix servers on your network from a single point without manual intervention. You can install applications on servers regardless of their physical locations, network connection type, or individual hardware setup.

Citrix IMS uses Published Application Manager to push application installations to your Citrix servers and also to uninstall those applications if necessary: publishing a Citrix IMS application causes each server configured to run the application to download and install the application while deleting a published IMS application causes each server configured to run the application to uninstall the application.

Load Balanced Applications

Published Application Manager supports publishing of an application on multiple servers if Citrix Load Balancing Services is installed on those servers.

When an ICA Client user connects to a published application configured to run on multiple servers, load balancing determines which server will run the application based on server load. The ICA Client contacts the master ICA Browser, which maintains a list of servers configured to run the published application, to find the address of a server containing the published application.

The master ICA Browser selects one of the servers based on load and returns the address of that server to the ICA Client.

You can tune how load balancing support calculates server load for each server in a load balancing server farm using the Load Balancing Administration utility. For instructions on balancing application load, see Chapter 6, "Advanced Topics."

Videos

In order to publish videos, you must install Citrix VideoFrame on your network. Viewing a published video requires the same published application connection procedure used by standard published applications. When a user connects to a published video, the ICA Client connects to a MetaFrame server configured to run the video, determines the location of the video, and then launches the Windows Media Player, which plays the video from the VideoFrame server.

Note Playing videos requires the Citrix ICA Client for Win32 (Program Neighborhood) and Microsoft Windows Media Player.

Scopes of Management

You can publish and manage applications using one of two management scopes: server farms or the Windows NT domains.

Important In order to take advantage of the features of Program Neighborhood and the administrative organization of the server farm, you must publish and manage your applications using the server farms management scope.

Use the Windows NT domains scope only if you:

- Cannot add your servers to a server farm
- Need to maintain applications that were both published prior to installation of MetaFrame 1.8 and cannot be migrated into a server farm

Server Farms Scope

When you use the server farms scope of management, you group your Citrix servers (MetaFrame 1.8 and *WINFRAME* 1.8) into one or more server farms. When creating a server farm, keep the following in mind:

- **Common administrator's rights**. The individuals responsible for administration of a farm should have administrative rights over each server in the farm. When you log into a Citrix server console or ICA session and run Published Application Manager, you administer applications under the context of your current Windows NT user name. Although you can view the applications on other servers in the farm without having administrative rights over those servers, you cannot publish or edit applications on those servers. For this reason, users who must run Published Application Manager to publish applications should make sure they have administrative privileges on each server in the farm.
- **Common base of user accounts**. Server farms can include servers, and therefore users, from multiple domains. All ICA Client users must belong to a group of users common to all involved domains. Published Application Manager draws a common user account base from the intersection of the trust relationships of all affected Windows NT domains. See "Trust Intersection" below for more information on determining a common base of user accounts.
- **Physical Connection**. Servers in a farm must be connected by some form of network connection. Some possible network connections include LAN, WAN, and dial-up asynchronous connections. Servers can be on different subnets if an ICA Gateway is in place to connect them. ICA Gateways are administered from Citrix Server Administration. See "Connecting Citrix Servers Across Network Subnets" in Chapter 4, "Configuring MetaFrame" for more information.

Trust Intersection

The way you group servers into server farms depends on having a common base of user accounts among all involved Windows NT domains.

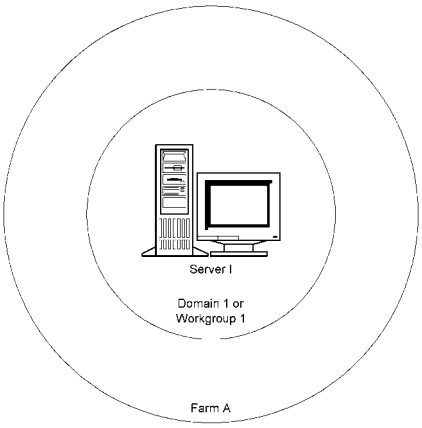
The common base of user accounts is determined by the intersection of the underlying trust relationships among the domains. For example, a farm can contain servers from:

A single domain named A	The trust intersection of A is A. You can configure published applications for all of A's users. This model works for a single server that is a member of a Windows NT domain, multiple servers that are members of a single Windows NT domain, as well as a single server that is a member of a Windows NT workgroup.

Two domains, named A and B	Domains A and B have a one-way trust relationship in which domain A trusts B. The trust intersection of these two domains is B. You can configure published applications for all user accounts on domain B. Note that a server that is a member of a Windows NT workgroup can never belong to a multiple server farm because there is no trust intersection between a workgroup and a domain.
Two domains, named A and B	Domains A and B have a two-way trust relationship in which domain A trusts B and domain B trusts A. The trust intersection of these two domains is A and B. You can configure published applications for all user accounts on domains A and B.
Three domains, named A, B, and C	Domains A and B have a one-way trust relationship in which domain A trusts B. A server from a third domain, named C, is added to the farm. C has a one-way trust relationship with B, in which C trusts B. The trust intersection of these three domains is B. You can configure published applications for all user accounts on domain B.
Three domains, named A, B, and C	Domains A, B, and C participate in a master domain model network in which domain A is the master domain and B and C are subordinate domains. According to the master domain model, domains B and C each have a one-way trust with domain A in which domain B trusts A and domain C trusts A. The trust intersection of these three domains is A. You can configure published applications for all user accounts on domain A. This scenario works with multiple master domains as well.

Server Farm Arrangements

You can configure your server farms in multiple ways depending upon your needs and the existing structure of your network. The following diagrams illustrate some of the ways you can arrange Citrix servers in server farms.



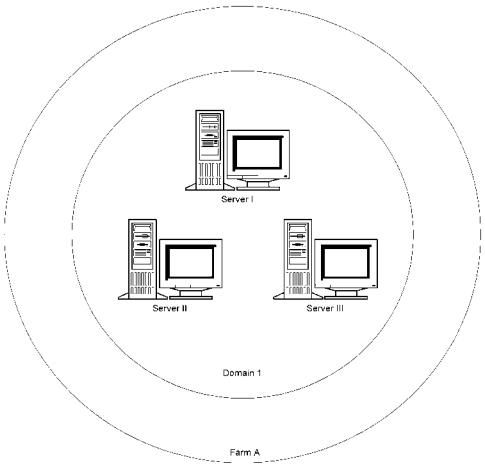
The farm depicted above contains either a single server in a Windows NT domain or a single server in a Windows NT workgroup.

Put a single domain-based or workgroup-based server in a farm so that you can take advantage of server farm administrative and Program Neighborhood features.

A farm containing a server that is a member of a Windows NT workgroup can contain only one server. This limitation exists because a workgroup-based server, which uses local user accounts only and does not share account information with other servers, cannot share a common base of user accounts with another server.

The user account base of a single server farm is comprised of all domain user and user group accounts (in the case of a single-server farm containing one domain-based server) or all local user and user group accounts (in the case of a single-server farm containing one workgroup-based server).

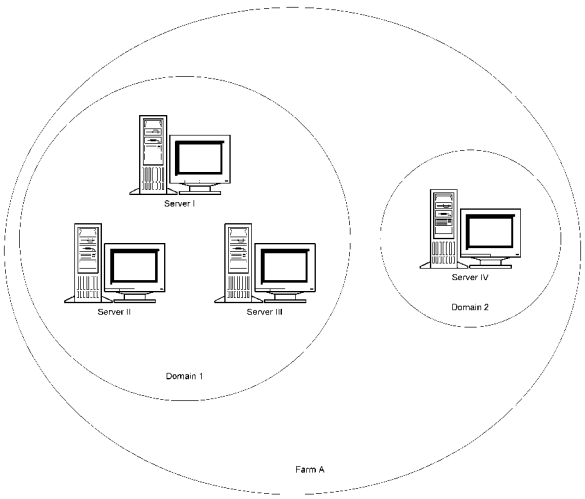
A farm containing a single server that is a member of a Windows NT domain can expand to contain additional servers:



The farm depicted above contains multiple servers from a single Windows NT domain. The user account base for this farm is simple: when you publish an application in this farm, you can grant access to any desired domain user or user group.

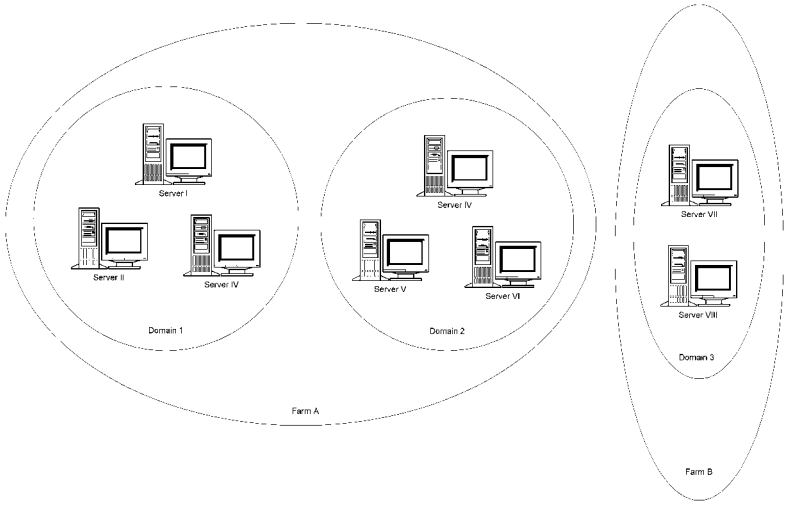
Note You cannot use each server's local user or user group accounts when publishing applications. Local user accounts cannot be part of a base of common user accounts.

The following farm contains multiple servers in multiple Windows NT domains:



Server farms can include multiple domains as long as a common base of user accounts exists between the domains. In the example above, the trust relationship between Domain 1 and Domain 2 determines the user account base.

Each domain can contain a single or multiple servers. As with a farm containing multiple servers from a single domain, a multiple domain farm cannot include workgroup servers and cannot include user accounts local to each server in the base of user accounts.



If necessary, you can create multiple farms on your network. Multiple farms are administered independently of each other—no published application information is shared between farms.

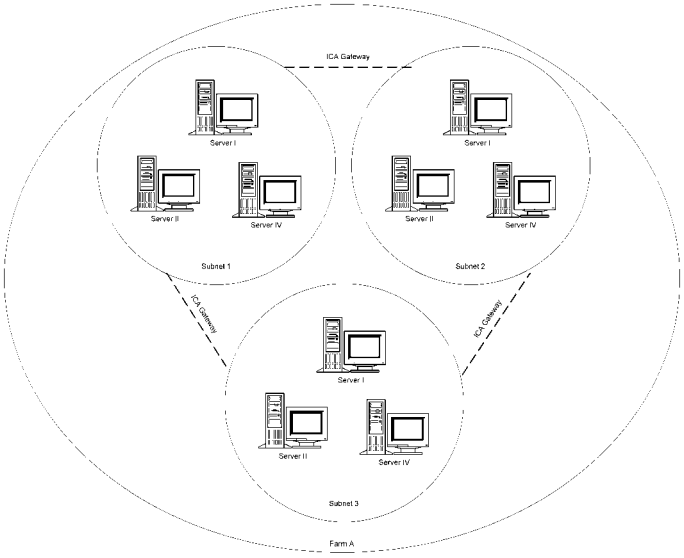
Some reasons why you might want to create multiple farms include:

Accounting and charge-back	If you track resource utilization in order to charge separate departments, you can create separate farms for the respective departments.
Geographical split	Although farms can span a geographical split, it may not be practical from an administrative point of view to create a single farm that must be administered by two IT groups in two different locations.
Lack of common user account base	If your Citrix servers must provide applications to groups of domain users that cannot comprise a single common user account base (the involved domains cannot trust each other), you must create separate farms.

Tip You do not have to create separate server farms to deliver different applications to different user groups in the common account base. Although each application you publish is published in the server farm, each user in the common account base sees only the applications he or she is authorized to use.

Multiple farms do not have to include multiple domains; you can create multiple farms containing servers that are members of a single domain. Each server can be a member of a single farm only.

In any farm arrangement, you can create a farm that consists of servers located on separate network subnets:



The farm depicted above contains servers from three separate subnets. In order for servers on different subnets to participate in a single server farm, you must set up an ICA Gateway between each subnet.

An *ICA Gateway* is a Citrix server communication link established between two subnets that allows the master ICA Browsers on the separate subnets to share information about available Citrix servers and published applications.

Note Like Windows NT domain trust relationships, ICA Gateways are not transitive. Each subnet must be connected to each other subnet by an ICA Gateway. To connect two subnets, you must create a single ICA Gateway. To connect three subnets, create three ICA Gateways.

See Chapter 4, "Configuring MetaFrame" for information on configuring ICA Gateways.

Windows NT Domains Scope

If you do not add your servers to a Citrix server farm, Published Application Manager functions in the Windows NT domains scope of management. In this scope, the applications you publish do not support Program Neighborhood features.

The Windows NT domains scope exists for backward compatibility and interoperability with existing *WINFRAME* 1.7 and MetaFrame 1.0 installations.

Configuring Server Farms

Setting up a server farm requires little configuration. Published Application Manager includes a wizard that lets you individually enter servers into a farm. Once you place your server(s) in a farm, you do not have to perform any additional administrative duties related to administering the farm structure itself.

Joining a Server Farm

If a Citrix server is not a member of a farm, you can add it to a farm at any time.

▶ **To join a server farm**

1. Start Published Application Manager on the computer you want to enter into a server farm. You can run Published Application Manager from the console or in an ICA session on the server.
2. From the **Configure** menu, click **Join Server Farm**.
3. The Join Citrix Server Farm wizard appears. Click **Help** in any screen of the wizard for additional help.

If you published applications on the server before putting it in a server farm, see "Migrating Applications to a Server Farm" below for information on converting those applications to server farm applications.

Migrating Applications to a Server Farm

Applications created under the Windows NT domains management scope do not have Program Neighborhood capabilities. You can use the Server Farm Application Migration wizard to convert Windows NT domains published applications into server farm published applications. Migrating an application into a server farm makes the application Program Neighborhood-capable. After migrating an application, you can edit the application's properties to configure Program Neighborhood functions.

Use the Server Farm Application Migration wizard after placing a server with an existing base of published applications into a farm for the first time or after upgrading a pre-MetaFrame 1.8 server containing previously published applications to MetaFrame 1.8.

Note The server (or servers, in the case of a load balanced application) containing the published application(s) you want to migrate must already be a member of a farm before you can migrate its published applications. See "Joining a Server Farm" earlier in this chapter for information on how to join a server farm.

▶ **To migrate a published application to a server farm**

1. Make sure you are in the server farm management scope. (From the **View** menu, click **Select Scope**. In the dialog box that appears, click the **Within a Citrix server farm** radio button. In the **Select a Citrix server farm** pull-down list, select the farm of which the server containing the published application to migrate is a member.)
2. Make sure you are viewing the server that contains the published application you want to migrate. (From the **View** menu, click **Select Server**. In the dialog box that appears, select the server from the list and click **OK**. If the server does not immediately appear in the list, click **Refresh Server List**.)
3. Select the published application in the main window and from the **Application** menu, click **Migrate**, or right-click the published application and click **Migrate**. The Server Farm Application Migration wizard appears. Click **Help** in any screen of the wizard for additional help.

After migrating an application, you can edit the application's properties to configure Program Neighborhood connection properties and requirements. See "Maintaining Published Applications" for information on changing a published application's properties.

Changing Farm Membership

You can change server farm membership for individual servers using the Change Server Farm wizard. This wizard lets you move a server from its current farm to an existing or new farm. You cannot remove a server from a farm altogether.

Note If the server whose membership you want to change has any load balanced applications with other servers in its current farm, you must remove the server from the list of servers configured for those applications before changing its membership. See "Maintaining Published Applications" for information on changing the list of servers configured to host the application.

▶ **To change farm membership**

1. Make sure you are in the server farm management scope. (From the **View** menu, click **Select Scope**. In the dialog box that appears, click the **Within a Citrix server farm** radio button and then select the farm of which the server is a member in the **Select a Citrix server farm** pull-down list.)
2. Make sure you are viewing the server whose membership you want to change. (From the **View** menu, click **Select Server**. In the dialog box that appears, select the server from the list and click **OK**. If the server does not immediately appear in the list, click **Refresh Server List**.)
3. From the **Configure** menu, click **Server Farm**. The **Server Farm Properties** dialog box appears.
4. Click **Change Server Farm**. The Change Server Farm wizard appears. Click **Help** in any screen of the wizard for additional help.

Creating a New Server Farm

You can create a new farm in one of two ways:

- Start Published Application Manager on a Citrix server that is not a member of a farm. The first time you start Published Application Manager, the Join Citrix Server Farm wizard appears. When asked to select a farm to join, specify a new farm name in the text field. If you choose to exit the wizard without joining a farm, the Join Citrix Server Farm wizard can be accessed at a later time by clicking **Join Server Farm** in the **Configure** menu.
- Change the membership of a server from an existing farm to a new farm. Use the Change Server Farm wizard and when prompted, specify a new farm name instead of selecting an existing farm. See “Changing Farm Membership” above for more information on starting the Change Server Farm wizard.

Viewing Servers and Published Applications

Published Application Manager’s main window displays a list of applications published on your Citrix servers. In order to provide flexibility and the ability to administer applications on servers other than the server on which it is running, Published Application Manager lets you select and filter the currently viewed server or servers.

The following topics describe how to view the servers and published applications you want to administer.

Selecting a Scope of Management

The **Select Scope** menu option lets you switch between Published Application Manager's two scopes of management: Citrix server farms and Windows NT domains.

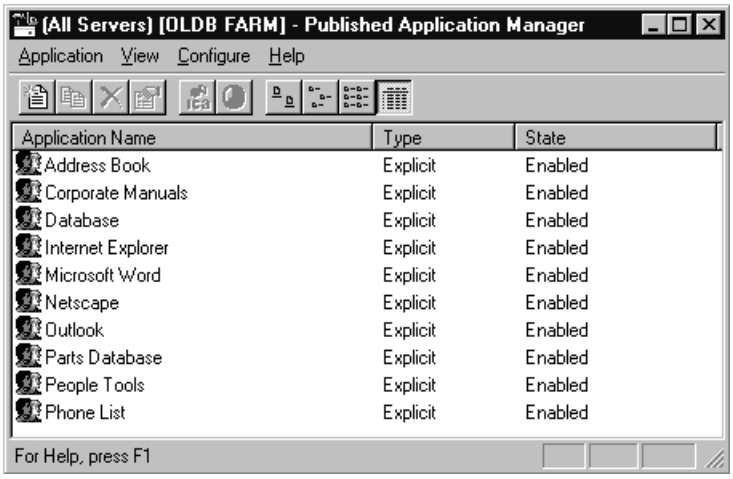
▶ **To select a scope of management**

1. From the **View** menu, click **Select Scope**. The **Select Management Scope** dialog box appears.
2. To publish applications in a server farm, click **Within a Citrix server farm**. The **Choose Server Farm** panel appears in the bottom half of the dialog box. Select a server farm from the list.
3. To publish applications in a Windows NT domain context, click **Using Only NT Domains**. The **Choose NT Domains** panel appears in the bottom half of the dialog box. Select a single, multiple, or all displayed domains.
4. Click **OK**. The Published Application Manager main window appears. The displayed applications are those hosted by server(s) in either the specified server farm or Windows NT domain(s).

You can now begin to edit existing applications or publish new ones. If you selected the server farm scope, all applications you publish will support Program Neighborhood features.

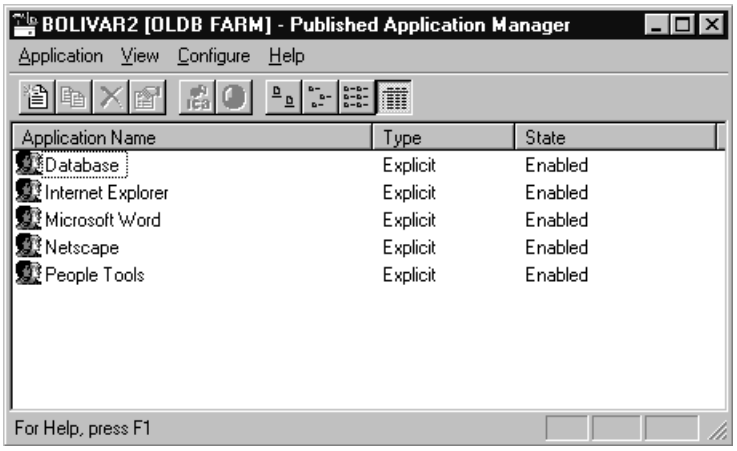
Selecting a Server to View

The currently displayed list of applications depends in part upon the servers being viewed. For example, if you are using the server farm scope of management to view all servers in a farm, the application list includes all applications published on the servers that make up the farm:



The main window's titlebar displays the currently selected server or servers. In this case, **All Servers** indicates that the current view displays all applications configured on all servers in the OLDB Farm.

If you are using the server farm scope of management to view a selected server in a farm, the application list includes only those applications published on that server:



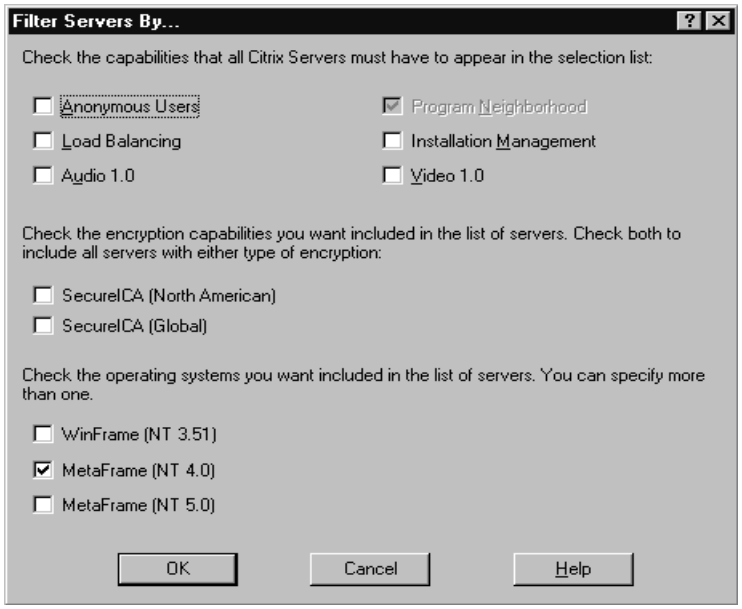
In this case, the applications configured on OLDB Farm's server Bolivar2 are displayed.

▶ **To select a server**

1. From the **View** menu, click **Select Server**.
2. In the **Select Citrix Server** dialog box, select the desired server from the list or select **All Servers**. You can also click **Filter Servers By…** to narrow down the list of servers according to specifiable criteria. Click **OK**.
3. The main window reappears displaying applications hosted by the specified server(s). The main window's titlebar displays the name of the currently selected server, or **All Servers** if you are viewing all servers, or **All Filtered Servers** if you filtered your view.

Filtering the Servers in Your View

Published Application Manager includes a filtering utility that lets you narrow your view of applications based upon certain specifiable criteria including server capabilities, supported encryption levels, and operating system type of the servers hosting the applications.



The criteria displayed above can be selected individually or in combination to produce a filtered server list. Filtered server lists show only applications that are hosted by servers that meet your specified requirements.

For example, filtering the view pictured in Figure 1 below, which displays all servers in a server farm, to display only applications configured on *WINFRAME* servers in the farm, results in the view in Figure 2:

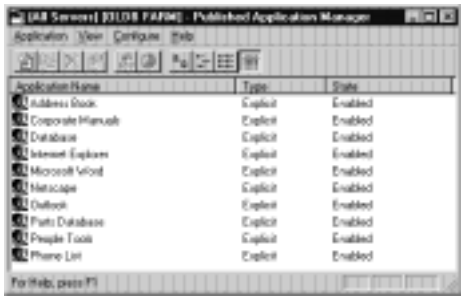


Figure 1

Figure 2

▶ **To filter servers**

1. From the **View** menu, click **Select Server**.
2. In the **Select Citrix Server** dialog box, click **Filter Servers By**. The **Filter Servers By** dialog box appears. Select the criterion, or criteria, by which you want to filter your servers. For example, if you select **Load Balancing** and **SecureICA (North American)**, the applications displayed are those running on servers with SecureICA Services North American version and Load Balancing Services installed.
3. After selecting the desired capabilities and requirements, click **OK**. You are returned to the **Select Citrix Server By** dialog box. The servers in the list meet the specified criteria. Select the individual servers or **All Filtered Servers** and click **OK**. When you return to Published Application Manager's main window, the applications displayed are those that are hosted by servers that meet your requirements.

Publishing Applications

The following topics describe how to configure four different types of published application: standard, video, Citrix IMS, and load balanced.

Before publishing applications, please review the following information on configuring users and user groups for access to published applications.

Configuring Users

Before publishing applications, consider your base of ICA Client users and the Windows NT user accounts they must use to access the applications you publish. Application Publishing provides ICA session access to two types of user accounts: anonymous and explicit.

Note The total number of users, whether anonymous or explicit, who can be logged on to the MetaFrame server at the same time is contingent upon your licensed user count.

Anonymous Users

During MetaFrame installation, the Setup program creates a special user group called *Anonymous*. By default, this Citrix-created Windows NT user group contains 15 user accounts with account user names in the format Anon*x*, where *x* is a number in the form 000, 001,... up to 015. Anonymous users have guest permissions by default.

If an application published on the Citrix server can be accessed by guest-level users, the application can be configured (using Published Application Manager) to allow access by anonymous users. When a user starts an anonymous application, the Citrix server does not require an explicit user name and password to log the user onto the server, but selects a user from a pool of anonymous users who are not currently logged on.

Anonymous user accounts are granted minimal ICA session permissions. Anonymous user ICA connection permissions include the following properties that differ from standard ICA session permissions for the default user:

- Ten minute idle (no user activity) timeout
- Logged off on broken connection or timeout
- No password is required
- User cannot change password

Anonymous user accounts do not have a persistent identity; no user information is retained when an anonymous user session ends. Any desktop settings, user-specific files, or other resources created or configured by the ICA Client user are discarded at the end of the ICA session.

Note Anonymous users are not supported on a Citrix server configured as a primary or backup domain controller.

The 15 anonymous user accounts created during MetaFrame installation usually do not require any further maintenance but their properties can be modified using User Manager for Domains.

Adding and Modifying Anonymous Users

If you install additional user licenses, anonymous users are not automatically created. Adding anonymous users is simply a matter of creating new users and assigning them to the Anonymous group. For security reasons, these user accounts should not belong to any other groups. The easiest way to create additional anonymous users is to copy an existing anonymous user account.

▶ **To add anonymous users**

1. Run User Manager for Domains: on the MetaFrame desktop, click **Start**, point to **Programs**, point to **Administrative Tools**, and click **User Manager for Domains**.
2. In the **User** menu, click **Select Domain**.
3. Enter the computer name of the Citrix server in **Domain** and click **OK**.
4. Select an existing anonymous user.

5. In the **User** menu, click **Copy**.
6. Enter a unique name in **Username** and click **Add**.

   Though not a requirement, it is best to use names of the form Anon*xxx*, following the pattern of the existing anonymous users. (You can use any name as long as the user is part of the Anonymous group.)
7. Repeat to add multiple users.
8. After the last anonymous user is added, click **Close**.
9. Exit User Manager for Domains.

   The new user accounts are not available until the MetaFrame server is rebooted.

Use the following procedure to change settings for anonymous users.

▶ **To modify anonymous user settings**

1. Run User Manager for Domains.
2. In the **User** menu, click **Select Domain**.
3. Type the computer name of the MetaFrame server in **Domain** and click **OK**.
4. Select the anonymous users.
5. In the **User** menu, click **Properties.**
6. Change the properties as desired.
7. Click **OK** in the **User Properties** dialog box.
8. Exit User Manager for Domains.

Explicit Users

An *explicit* user is any conventional MetaFrame user who is not a member of the Anonymous group. Explicit users are created and maintained with User Manager for Domains. Explicit users have a “permanent” existence: their desktop settings, security settings, etc. are retained between sessions for each user in a user profile. Explicit users can be of any user class and are generally created for a specific purpose.

Note Never assign an explicit user to the Anonymous group.

Security Considerations

In addition to using standard Windows NT security features and practices, access to Citrix servers can be restricted in several ways:

- All users on a specific connection type can be restricted to running published applications only. By allowing users to access predefined applications only, you can prevent unauthorized users from obtaining access to the Windows desktop or a command prompt. Use the **Advanced Connection Settings** dialog box in Citrix Connection Configuration to restrict users to running only published applications.
- Published Application Manager lets you restrict an application to specified users or groups of users (explicit user access only).
- MetaFrame supports Internet firewalls that can be used to restrict Internet access to the MetaFrame server.
- Users can be required to enter a user name and password in order to execute an application (explicit user access only).
- Citrix and most Web professionals recommend you either disassociate your Web site from your production system or rigorously restrict external access. Any system accessible through the Internet is by definition a security risk and may give anyone unauthorized access to your production site through the Web. Therefore, unless you have very robust security and plan to use this with an Intranet, keep your Web server on a separate network loop outside your firewall, if you have one.
- The Aclcheck utility examines the security ACLs associated with your files and directories and can report on any potential security exposures. See Appendix A, "MetaFrame Command Reference," for more information about this command.
- The Application Execution Shell (App) lets you write application execution scripts that perform actions before executing the application and perform cleanup after the application terminates. See Appendix A, "MetaFrame Command Reference," for more information about this command.

Publishing a Standard Application

Once you enter your server(s) into a server farm, you can begin to publish applications in the farm. Applications published in a farm automatically appear in each specified Program Neighborhood user's application set and are pre-configured for such session properties as window size and colors and supported level of encryption, audio, and video. Non-Program Neighborhood ICA Clients will also have access to these applications: these ICA Client users can create connections to the published application using their connection configuration managers or can access the published application over the Internet or Intranet (in the case of the ICA Web Clients).

▶ To publish an application in a server farm

In order to publish an application in a server farm, the server or server which is to host the application must be a member of a farm. Make sure the server is a member of a farm before attempting to publish the application. See "Joining a Server Farm" earlier in this chapter for more information.

1. Make sure you are in the server farm management scope. (From the **View** menu, click **Select Scope**. In the dialog box that appears, click the **Within a Citrix server farm** radio button and then select the farm of which the server is a member in the **Select a Citrix server farm** pull-down list.)
2. Make sure you are viewing the server on which you want to publish the application. (From the **View** menu, click **Select Server**. In the dialog box that appears, select the server from the list and click **OK**. If the server does not immediately appear in the list, click **Refresh Server List**.)
3. From the **Application** menu, click **New** to start the Application wizard. Click **Help** in any screen of the wizard for additional help.

Note In addition to specific applications, you can also publish a Citrix server desktop. When users connect to published applications configured as desktop sessions, the users are presented with a standard Windows NT desktop. Publishing a desktop session provides redundancy and scalability. Users can access Windows NT desktops without knowing individual server names. In addition, servers can be added to a server farm and capacity increased without reconfiguring user connections. Configure a desktop session by creating a published application without specifying a command line and working directory.

Published Application Manager includes the Windows NT domains scope of management to provide backward compatibility and interoperability with existing Citrix server installations (*WINFRAME* 1.7 and MetaFrame 1.0) that contain existing published applications. Using Published Application Manager to publish applications in this scope results in applications that are not enabled for automatic configuration of Program Neighborhood sessions.

▶ To publish an application on a non-server farm server

1. Make sure you are in the Windows NT domains management scope. (From the **View** menu, click **Select Scope**. In the dialog box that appears, click the **Using only NT Domains** radio button and then select the domain on which the server is a member in the domain list.
2. Make sure you are viewing the server on which you want to publish the application. (From the **View** menu, click **Select Server**. In the dialog box that appears, select the server from the list and click **OK**. If the server does not immediately appear in the list, click **Refresh Server List**.)
3. From the **Application** menu, click **New** to start the Application wizard. Click **Help** in any screen of the wizard for additional help.

Publishing a Video

Before publishing a video, you must encode the video using the Citrix VideoFrame Encoder and then copy the video (.avi) file to a VideoFrame server.

▶ **To publish a video**

1. Use the standard application publishing wizard to publish a video. (From the **Application** menu, click **New**.) If you are viewing more than one server when you start the wizard, you are asked to select a default server for the video. Select any server in the farm or domain.
2. Proceed through the wizard as usual until you reach the **Define the Application** screen. In the **Command Line** field, enter the full path and file name of the Citrix Video Information (.cvi) file for the video. You can type a Universal Naming Convention (UNC) name or network drive and full path or click **Browse** to locate the server that contains the .cvi file. In the **Choose Application** dialog box that appears, select **VideoFrame Information files** from the **Files of type** list box and then locate and select the .cvi file.
3. Proceed through the remainder of the wizard as usual.

Publishing a Citrix IMS Application

In order to use Published Application Manager to deploy an application to your Citrix servers, you must install Citrix IMS components on your network and use them to package the application for deployment. For more information on Citrix Installation Management Services, see the *Citrix Installation Management Services Administrator's Guide.*

Before publishing a packaged application, make sure the IMS script and package for the application are stored in the same directory on your file server and that the file server is accessible to all Citrix servers running Installation Management Services.

▶ **To publish a Citrix IMS application**

1. Use the standard application publishing wizard to publish an IMS application. (From the **Application** menu, click **New**.) When you start the wizard, you are asked to select a default server for the application if you are currently viewing more than one server. Select any server in the farm or domain and proceed.
2. Proceed through the wizard as usual until you reach the **Define the Application** screen. In the **Command Line** field, enter the full path and file name of the IMS script for the application you want to install on your Citrix servers (IMS scripts have a .wfs file extension).

You can type a UNC name or network drive and full path or click **Browse** to locate the file server that contains your IMS script and package. In the **Choose Application** dialog box that appears, select **IMS Scripts** from the **Files of type** list box and then locate and select your script.

3. Proceed through the wizard as usual until you reach the **Add the Application to Citrix Servers** screen. Click **Filter Servers By**. In the **Filter Servers By…** dialog box, check **Installation Management**. When this option is checked, the Citrix servers that appear in the **Available** list in the **Add the Application to Citrix Servers** screen are only those that have the IMS Installer and a Citrix Installation Management Services license installed. Click **OK**. In the **Available** list, select the Citrix servers on which you want to install the application and click **Add**.

Publishing a Load Balanced Application

In order to publish a load balanced application, you must install Citrix Load Balancing Services on each server you want to host the application. For more information on Citrix Load Balancing Services, see Chapter 6, "Advanced Topics."

▶ **To publish a load balanced application**

1. Use the standard application publishing wizard to publish a load balanced application. (From the **Application** menu, click **New**.) When you start the wizard, you are asked to select a default server for the application if you are currently viewing more than one server. Select any server in the farm or domain and proceed.
2. In the **Add the Application to Citrix Servers** screen of the wizard, you can specify multiple servers to run the session. If Load Balancing Services is not installed, only the current server is displayed in the **Configured** list and the **Add** button is unavailable.
3. Use the **Edit Configuration** button in the **Add the Application to Citrix Servers** screen to individually specify command lines and working directories on servers that have the application installed in a directory structure that differs from the installation on the default server.

Note Publishing an application on multiple load balanced servers without specifying a working directory or command line for the application creates a load balanced Citrix server desktop. ICA Client users can connect to this type of published application and run any applications accessible from the desktop of the Citrix server.

Maintaining Published Applications

After you publish an application, you can later change its properties. Common reasons to change a published application's settings include when you want to:

- Rename the published application. This modification changes the name under which ICA Client users access the application.
- Change the list of users allowed to run the application.
- Change the list of Citrix servers hosting the application.
- Change the command line and working directory for the application. This modification alters the path information for the application's executable, IMS script (for Citrix IMS applications), or Citrix Video Information file (for published videos). You can also edit or add parameters to the command line when applicable.
- Change Program Neighborhood settings applied to this application when it is accessed by a Program Neighborhood (for applications created in the server farm management scope only).

Note The properties of applications published for a Citrix server farm (or migrated into a server farm) cannot be edited when viewed from the Windows NT domains scope (all tabs in the dialog box are grayed-out). To edit the application, you must change your scope to the Citrix server farm scope.

▶ **To change the properties of a published application**

- Select the entry for the published application. From the **Application** menu, click **Properties** or right-click an entry and click **Properties**. Click **Help** in any tab of the **Properties** dialog box for additional help.

Enabling and Disabling Published Applications

When you publish an application, it is enabled by default. Enabled applications are available to the users you specify in the new application wizard. You can also temporarily disable your published applications. Disabling an application makes it unavailable to ICA Client users until you re-enable it.

▶ **To disable an application**

- Select the entry for the published application. From the **Application** menu, click **Disable** or right-click an entry and click **Disable**.

▶ **To enable an application**

- Select the entry for the published application. From the **Application** menu, click **Enable** or right-click an entry and click **Enable**.

Deleting Published Applications

Deleting a published application removes all published application configuration information from each server in the published application's list of configured servers. When you delete a published application, the application referenced by the published application is no longer available to ICA Client users under the published application name (although it may be available as another published application or from a Citrix server desktop session). If you want to make the application available again either under its old name or with a new name, simply republish it.

Note The effects of deleting a Citrix IMS application differ from those of deleting a standard application. When you delete an entry for a Citrix IMS application, Published Application Manager actually uninstalls the application on the specified server(s).

▶ **To delete a published application**

- Select the entry for the published application. From the **Application** menu, click **Delete** or right-click an entry and click **Delete**.

CHAPTER 6

Advanced Topics

Overview

This chapter discusses advanced MetaFrame system administration topics. Topics discussed include:

- Understanding MetaFrame Load Balancing
- MetaFrame Security Tools
- Using ICA with Network Firewalls
- General Tips and Troubleshooting

Understanding MetaFrame Load Balancing

Load balancing allows an application to be published for execution on any of several Citrix servers in a server farm. When a published application or desktop session configured for multiple servers is launched from a Citrix ICA Client, load balancing selects which server will run the application or desktop session based on server load. You can tune how load balancing calculates server load for each server in a server farm using the Load Balancing Administration utility.

The Citrix ICA Client contacts the master ICA Browser to find the address of a server containing the published application. The master ICA Browser maintains a list of servers configured to run the published application. The master browser selects one of the servers based on load and returns the address of that server to the Citrix ICA Client. Each server calculates a separate load level for each network protocol (IPX, TCP/IP, and NetBIOS).

Load balancing supports mixing *WINFRAME* 1.7 or later and MetaFrame servers in a single server farm. Load-balanced applications must be installed on each server in the farm.

Use Published Application Manager to configure published applications. See Chapter 5, "Publishing Applications," for more information.

Note Load balancing is available only when a copy of Citrix Load Balancing Services has been installed on each server that will participate in load balancing.

Reconnecting to Load Balanced Sessions

Published applications allow a user to run applications or access a desktop session without knowing the name or address of a particular server. If the published application is located on a single server, the user can disconnect and reconnect to the same session.

If the published application is configured to run on multiple servers in a server farm, the user must be reconnected to the same server in the server farm to reconnect to his or her session. The ICA Browser can reconnect the user to his or her previous session on the same server under certain conditions.

When the user attempts to reconnect to the published application, the ICA Client queries the master ICA Browser for the address of the published application. The master ICA Browser checks the list of disconnected sessions. If it finds a disconnected session from the same ICA Client, it returns the address of the server with the disconnected session.

To reconnect to disconnected load balanced sessions, the following criteria must be met:

- The user must disconnect gracefully from the server; for example, by clicking **Disconnect** from the **Start** menu.
- The user must reconnect from the same Citrix ICA Client computer (using the same client name).

You can use **query server /disc** to view a list of disconnected sessions.

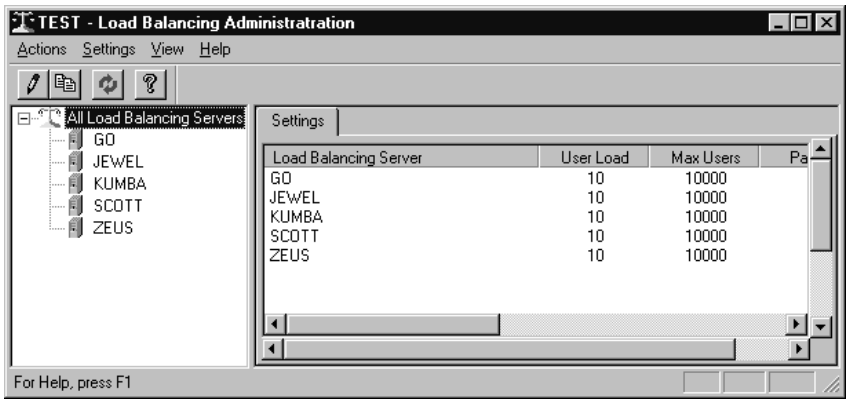
Note If users frequently disconnect and reconnect their sessions rather than logging off, the number of sessions on a server farm may not be evenly distributed because users are reconnected to their previous session on the same server.

Tuning Load Balancing

Tuning the load balancing calculations allows servers with different performance capabilities to evenly distribute Citrix ICA Client sessions. The load calculation is tuned separately for each server. Use the Load Balancing Administration utility to tune load balancing parameters.

▶ **To tune server load balancing parameters**

- Click **Load Balancing Administration** in the **MetaFrame Tools** menu. The **Load Balancing Administration** screen appears:



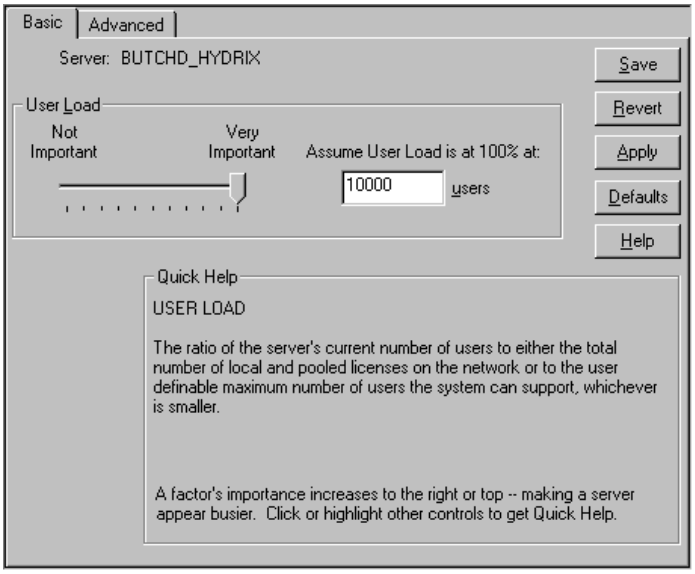
The **Settings** tab displays the current load balance parameters for each load balancing server when **All Load Balancing Servers** is selected in the left pane.

You can tune how load balancing support calculates server load for each server in a load balancing farm. You can copy the settings for one server to another server.

Click a server to display the **Basic** and **Advanced** load balance parameters.

▶ **To adjust basic load balancing settings**

- Click a Citrix server in the server list pane. The **Basic** load balance settings tab for the selected server appears in the right pane:



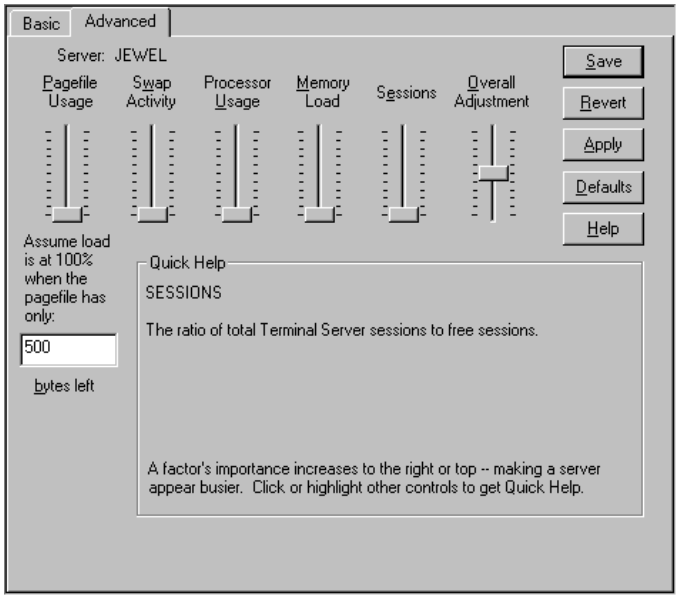
▶ **To balance two or more servers in a Load Balancing farm**

1. Determine how many users each server can support.
2. Click on the *servername* in the left pane and then click the **Basic** tab.
3. Enter the number of users determined in Step 1 in the **Assume User Load is at 100% at *x* users** box.
4. Set **User Load** at **Very Important**.
5. Click **Save**.
6. Repeat for each server in the farm.

   Click **Save** to keep the adjustments for this server. Click **Revert** to discard any changes made.

▶ **To adjust advanced load balance parameters**

1. Click on the *servername* in the left panel and then click the **Advanced** tab.



2. Set the importance factor for each load balancing parameter.
3. Click **Save**.
4. Repeat for each server in the farm.

Adjusting a Server's Load Balance Calculation

Use Load Balancing Administration to adjust six factors that influence the calculation of the overall server load. Each factor can be given a relative importance that controls how much influence that factor has when calculating total load. An overall adjustment further raises or lowers a server's load calculation. The factors are:

- **User Load**. The ratio of the current number of users to the smaller of:
  - The total number of local plus pooled user counts on the network.
  - The maximum number of users the system can support.

    The *maximum number of users the system can support* is the smaller of:
    - The number of ICA connections per protocol. By default, the number of ICA connections for each protocol is unlimited on MetaFrame servers and two on *WINFRAME* servers.
    - A user definable number. By default, the user definable number is simply an arbitrarily large number.

- **Pagefile Usage**. The ratio of the current pagefile size to the allowed minimum free space left in the pagefile.
- **Swap Activity**. The number of times per second the pagefile is accessed.
- **Processor Usage**. The percent of time the processor is busy.
- **Memory Load**. The ratio of available memory to total physical memory.
- **Sessions**. The ratio of total configured ICA connections to free ICA connections.
- **Overall Adjustment**. Raises or lowers the overall calculated load of a server. By default, this is set at no adjustment.

Note Sessions that use RDP are not counted for the **User Load** or **Sessions** calculations. If you mix Citrix ICA and RDP connections, configure your servers to use advanced factors such as **Processor Usage** and **Memory Load** to calculate load level.

The Importance Settings

You can adjust the importance of each factor. The *importance* of a factor determines how much its load influences the overall system load calculation relative to the other factors. For example, if **User Load** is set at **Very Important** and all other factors are set at **Not Important**, the **User Load** calculation is the only factor used to determine overall system load.

Each of the importance settings is independent of the other settings. Raising the importance of one factor does not influence how important any other factor is in the overall calculation. For example, if each factor is set at very important, all factors are given the same weight.

Note If you want to temporarily prevent a particular Citrix server from being selected to run any load balanced applications, set all importance sliders for that server to **Not Important**.

Additional Settings

Two of the factors, **User Load** and **Pagefile Usage**, have additional parameters you can adjust.

User Load

User Load is the ratio of the current number of users to the smaller of:

- The total number of local plus pooled user counts on the network.

- The maximum number of users the system can support.

  The *maximum number of users the system can support* is the smaller of:

  - The number of ICA connections per protocol. By default, the number of ICA connections for each protocol is unlimited on MetaFrame servers and two on *WINFRAME* servers.
  - A user definable number. By default, the user definable number is simply an arbitrarily large number.

Specify a maximum number of users when you have servers capable of handling different numbers of users.

Suppose you have two servers, A and B. Testing shows that A can handle 100 concurrent users, while B can handle 50 concurrent users. By default, each server would get an equal number of users logging in.

By setting server B's **User Load** parameter at 50 and making the **User Load** factor **Very Important**, you force that server's user load calculation to be 100% when 50 users are logged on. This keeps servers A and B balanced so that B does not get more users than it can handle. At the same time A does not get fewer users than it can handle.

Note Sessions that use RDP are not counted for the **User Load** calculations. If you mix Citrix ICA and RDP connections, configure your servers to use advanced factors such as **Processor Usage** and **Memory Load** to calculate load level.

Pagefile Usage

Pagefile Usage is calculated by taking the ratio of the current pagefile size to the allowed minimum free space left in the pagefile. By default, the pagefile usage load equals 100% when the pagefile has 500 bytes free.

Adjust the minimum amount of free space for the pagefile usage load calculation in the **Assume load is at 100% when the pagefile has only *x* bytes left** box.

Advanced Factors

There may be situations where other factors besides **User Load** are helpful in calculating system load. For example, if the published applications you are using are very processor intensive, you may want to raise the importance of **Processor Usage** when calculating overall system load.

Warning Some adjustments may cause system load calculations to appear low when the server is actually running out of resources. Do not adjust these settings without a thorough understanding of how the advanced factors interact.

Click the **Advanced** tab to adjust the importance of advanced factors when calculating overall system load. The Importance factor for each parameter can be adjusted independently of any others.

MetaFrame Security Tools

In addition to the security issues common to Microsoft Windows NT Server, Windows Terminal Server has additional security issues related to *remote control*; that is, its ability to allow remote users to logon and execute applications remotely. This means that any remote users who logon to the server must be allowed to access files and directories in a secure fashion.

The MetaFrame security tools enhance the standard Windows Terminal Server security features by providing additional methods for securing file systems.

Using Aclset to Secure the File System

Aclset automatically secures all files and directories on all hard drives. Aclset secures *all* files, directories, and drives. After the file systems are secured, use the Security Configuration utility and other tools to selectively enable user access to files and directories. This method makes sure that there are no file system security holes. Aclset sets all file and directory Access Control Lists (ACLs) to grant Full Access rights to the Administrators and System groups only; the Users group is denied access. This step is also referred to as "locking down" the file system.

Warning Running Aclset denies user access to all files and directories on the Windows Terminal server. After running Aclset, users may not be able to logon and run any applications. Use Aclset only when a high security environment is required.

▶ **To use Aclset to secure the file system**

1. Start a Command Prompt session. Make sure no other programs or users are active.
2. At the command prompt, type **aclset** and press ENTER.
3. When Aclset is complete, the command prompt returns. There is no success message but any errors encountered are reported.

After Aclset completes, the file system is locked down. The Users group has no access to any drive, directories, or files. Running the Security Configuration utility unlocks selected system files and gives users limited access to selected directories (including users' home directories and temp directories).

The Aclcheck utility is used to display file and directory permissions that give excessive access to users and groups The Aclcheck utility can be used to verify the security of the MetaFrame server. See Appendix A, “MetaFrame Command Reference” for more information on using Aclcheck.

See the Windows Terminal Server documentation for information on using the Security Configuration utility.

Using the Application Execution Shell (App)

Many applications require write access to temporary files or directories to operate properly. Also, some applications use .INI files to define settings and preferences that are retained after the application terminates. Users may be able to change these preferences in undesired ways so that the next user who runs the application sees the settings left by the previous user instead of the standard settings.

One way to create a secure, standardized environment while allowing write access to files and directories is to use the Application Execution Shell utility (App). App lets you write execution scripts that copy standardized .INI files containing default settings to user directories before starting the application and that perform application-related cleanup after the application terminates.

App can also be used to create an execution script that is used in an .ICA file so that hackers cannot modify the execution parameters (for example, working directory or execution directory) because the parameters do not appear in the .ICA file, only the name of the App script file.

See Appendix A, “MetaFrame Command Reference” for more information on using App.

Auditing Logons

The **auditlog** utility is used to generate reports of logon and logoff activity. Auditlog can also display logon failures and session duration.

Auditlog processes the Windows NT Event Log. To use auditlog, you must enable Windows NT logon/logoff event logging with User Manager for Domains. See your Windows NT documentation for information on event logging.

See Appendix A, “MetaFrame Command Reference” for more information on the auditlog utility.

Using ICA with Network Firewalls

Network firewalls can allow or block packets based on the destination address and port. If you are using ICA through a network firewall, use the information provided in this section to configure the firewall.

ICA TCP/IP Connection Sequence

1. The Citrix ICA Client sends a packet to port 1494 on the Citrix server requesting a response to a randomly selected port above 1023.
2. The Citrix server responds by sending packets to the Citrix ICA Client with the destination port set to the port requested in Step 1.

If you have a firewall or other TCP/IP network security, configure it to allow TCP/IP packets on port 1494 to pass to Citrix servers on your network.

Configure the firewall to allow TCP/IP packet on ports above 1023 to pass to Citrix ICA Clients.

If the firewall is not configured to pass ICA packets, users may receive the error, "There is no route to the specified address."

Note You can configure the Citrix server to use a different port number than 1494. Use the **icaport** command-line utility to change the default port number on the server. For information about the **icaport** utility, see Appendix A, "MetaFrame Command Reference."

Citrix ICA Clients must be configured to use the new port. See the *Citrix ICA Client Administrator's Guides* for the clients you plan to deploy.

The ICA Browser

The ICA Browser service uses UDP port 1604. ICA Browser responses are sent to a high port number above 1023.

The firewall must be configured to allow inbound UDP port 1604 connections to Citrix servers for load balancing, server farms, and ICA server browsing to function correctly.

Warning Allowing untrusted access to the ICA Browser service entails some security risk. Configure the firewall to pass ICA Browser data only if load balancing and server browsing across the firewall are essential.

ICA Browsing With Network Address Translation

Some firewalls use IP address translation to convert private (Intranet) IP addresses into public (Internet) IP addresses. Public IP addresses are called “external” addresses because they are external to the firewall, whereas private IP addresses are said to be “internal” addresses.

Hosts on the internal network have one set of addresses that is translated to another set when passing through the firewall.

For example, an internal host has a private address 192.168.12.3. The firewall translates this into a different public address such as 206.103.132.20.

To browse Citrix servers and published applications, the Citrix ICA Client contacts a Citrix server and requests the address of the master ICA Browser. If the ICA Client is external to the firewall, it must be configured to use the public address of a Citrix server. The server returns the IP address of the current master ICA Browser to the ICA Client. By default, the IP address returned to the ICA Client is the internal address.

If the ICA Client is outside the firewall and the firewall is configured for address translation, the IP address returned to the client for the master browser will be incorrect.

Returning External Addresses to ICA Clients

Use the Altaddr utility to configure the ICA Browser server to return the external IP address to Citrix ICA Clients. You must configure every server that can be elected as the master ICA Browser.

The Altaddr utility sets an alternate address for the ICA Browser on that machine. The external address for the server is specified as the alternate address. The Citrix ICA Client requests the alternate address when contacting servers inside the firewall. The alternate address must be specified for each server in a server farm.

▶ **To set an alternate address for a Citrix server**

1. Determine the correct external IP address.
2. At a command prompt, type **altaddr /set *nnn.nnn.nnn.nnn***, where *nnn* is the alternate IP address determined in Step 1.
3. Repeat on each server.

See Appendix A, “MetaFrame Command Reference,” for more information on the Altaddr Utility.

In addition to specifying the alternate address on the Citrix server, the ICA Client must be configured to request the alternate address when contacting the master ICA Browser. For information on configuring ICA Clients to request the alternate address, see the *Citrix ICA Client Administrator's Guides* for the clients you plan to deploy.

General Tips and Troubleshooting

This section provides some tips and troubleshooting information for Citrix servers.

Applications Accessed On Network Drives

Citrix servers load only one instance of an executable image. The executable code is shared by every session running that application. If an application is loaded from a remote network drive and a network error occurs, the operating system assumes that the executable image is corrupt and does not allow further access to the application. All users must close the application and logout to restore access to the application.

To prevent applications from becoming unavailable due to network errors, make sure you install applications on a local disk.

TCP/IP Timeouts

If an ICA session over TCP/IP is interrupted due to a network error, TCP/IP can take a long time before detecting that the network connection has dropped.

Until TCP/IP times out, the session remains in an active state and the user cannot reconnect to it. You can work around this problem by setting an idle timeout on the TCP/IP ICA connection using Citrix Connection Configuration.

See the Citrix Connection Configuration online help for instructions.

APPENDIX A

MetaFrame Command Reference

Overview

This appendix describes the MetaFrame command line utilities. The commands listed in this appendix are:

- **aclcheck** (Security Audit Utility)
- **aclset** (Set Default Security ACLs)
- **altaddr** (Specify Alternate Server IP Address)
- **app** (Application Execution Shell)
- **auditlog** (Generate Logon/Logoff Reports)
- **change client** (Change ICA Client Device Mapping Settings)
- **cltprint** (Set the Number of Client Printer Pipes)
- **icaport** (Configure TCP/IP Port Number)
- **ndspsvr** (Enable or Disable a Preferred Server for NDS Logons)
- **query acl** (Security Audit Utility)
- **query license** (View MetaFrame Licenses)
- **query server** (View MetaFrame Servers)

ACLCHECK (Security Audit Utility)

Description

This command is identical to **query acl**. **Aclcheck** performs a file security audit on the specified directory or drive letter. **Aclcheck** reports file accesses allowed by accounts other than Administrator, Administrators, or SYSTEM. **Aclcheck** can also generate a report of registry keys that have Delete, Write, Add, Link, Change Permissions, or Take Ownership permissions for non-administrator users. The system security level (Low, Medium, or High) is also reported.

Syntax

aclcheck [*path*] [/**registry_only** | /**files_only** [/**ignore_execute**]] [/**?**]

Parameter

path
The name of the drive or directory path to audit.

Options

/registry_only
Checks only the system registry.

/**files_only**
Checks only disk files.

/**ignore_execute**
Do not report files with user Execute permissions.

/**?** (help)
Displays the syntax for the utility and information about the utility's options.

Remarks

Aclcheck generates a report of potential security exposures on a MetaFrame server. **Aclcheck** reports excessive file or registry accesses allowed by accounts other than Administrator, Administrators, and SYSTEM.

The file report shows any files that have Delete, Write, Append, Execute (unless the /**ignore_execute** option is specified), Change Permissions, or Take Ownership permissions for non-administrator users.

The registry report shows any registry keys that have Delete, Write, Add, Link, Change Permissions, or Take Ownership permissions for non-administrator users.

If no arguments are specified, **aclcheck** checks all local drives and then checks the **HKEY_LOCAL_MACHINE** portion of the system registry.

Any files or registry keys that non-administrator users can write to are reported in the following format:

```
OBJECT  INHERIT ACCOUNT       FILE
_______ _______ ____________ ____________________________________
DWXPO           \Everyone     C:\AUTOEXEC.BAT
X               \Everyone     C:\boot.ini
DWXPO           \Everyone     C:\CONFIG.SYS
X       X       \Everyone     C:\Wtsrv
```

Aclcheck also audits the MetaFrame execute list (created and maintained by the Application Security utility) to verify that no executable files in the execute list are writable by users.

ACLSET (Set Default Security ACLs)

Description

Aclset automatically secures all files and directories on all hard drives. **Aclset** secures **all** files, directories, and drives. After the file systems are secured, use the Security Configuration utility and other tools to selectively enable user access to files and directories. This method makes sure that there are no file system security leaks. **Aclset** sets all file and directory Access Control Lists (ACLs) to grant Full Access rights to the Administrators and System groups only; the Users group has no access. This step is also referred to as "locking down" the file system.

Warning **aclset** can irreversibly affect the operation of your MetaFrame server. Be sure to make a complete backup before securing your system.

Syntax

aclset [*path*]
aclset [/**?**]

Options

Type **aclset** with no parameters to secure all local drives.

path
The drive or directory to secure. The specified drive or directory and all subdirectories are secured.

/**?** (help)
Displays the syntax for the utility and information about the utility's options.

Remarks

Aclset with no parameters secures all files and subdirectories on all local drives by setting all files and subdirectories to administrator access only. Use this to perform the initial "lock down" on a server. After running **aclset**, use Security Configuration to configure Terminal Server operating system file and registry security. You must manually change the permissions on other files and directories as needed to provide user access.

ALTADDR (Specify Alternate Server IP Address)

Description

Altaddr is used to query and set the alternate (external) IP address that a MetaFrame server returns to clients who request it. The alternate address is an external address used by Citrix ICA Clients outside a firewall.

Syntax

altaddr [/**server**:*servername*] [/**set** *alternateaddress*] [/**v]**
altaddr [/**server**:*servername*] [/**set** *adapteraddress alternateaddress*] [/**v]**
altaddr [/**server**:*servername*] [/**delete**] [/**v]**
altaddr [/**server**:*servername*] [/**delete** *adapteraddress*] [/**v]**
altaddr [/**?**]

Options

/server:*servername*
Specifies the Citrix server on which to set an alternate address; otherwise the current Citrix server is used.

/set
Sets alternate TCP/IP addresses. If *adapteraddress* is specified, *alternateaddress* is assigned only to the network adapter with that IP address.

/delete
Deletes all alternate addresses on the specified server. If *adapteraddress* is specified, deletes only the alternate address for that adapter.

/v (verbose)
Displays information about the actions being performed.

/?
Displays the syntax for the utility and information about the utility's options.

Examples

Example 1: Set the alternate address to 1.1.1.1 for the current server:

```
altaddr /set 1.1.1.1
```

Example 2: Set the alternate address to 1.1.1.1 for the current server on the network interface card with *adapteraddress* 2.2.2.2:

```
altaddr /set 2.2.2.2 1.1.1.1
```

APP (Application Execution Shell)

Description

App is a script interpreter for secure application execution. **App** lets you write execution scripts that copy standardized .ini files containing default settings to user directories before starting the application and that perform application-related cleanup after the application terminates. The script commands are described below.

Syntax

app *scriptfilename*

Parameter

scriptfilename
The name of a script file containing **app** commands (see commands below).

Remarks

If no *scriptfilename* is specified, **app** displays an error message.

The Application Execution Shell reads commands from the script file and processes them in sequential order. The script file must reside in the %SystemRoot%\Scripts directory.

Script Commands

The script commands are:

copy *sourcedirectory\filespec targetdirectory*
Copies files from *sourcedirectory* to *targetdirectory*. *Filespec* specifies the files to copy, including wild cards (*,?).

delete *directory\filespec*
Deletes only files owned by the user in the *directory* specified. *Filespec* specifies the files to delete, including wild cards (*,?).

deleteall *directory\filespec*
Deletes all files in the *directory* specified. *Filespec* specifies the files to delete, including wild cards (*,?).

execute
Executes the program specified by the **path** command using the working directory specified by the **workdir** command.

path *executablepath*
Sets the program to be executed by *executablepath*.

workdir *directory*
Sets the default working directory to the path specified by *directory*.

Examples

The following script file runs the Solitaire card game, Sol.exe:

```
PATH C:\Wtsrv\System32\Sol.exe
WORKDIR C:\Temp
EXECUTE
```

The following script file runs the program Fubar.exe. It deletes files in the Myapps\Data directory created for the user that launched the application when the program terminates:

```
PATH C:\Myapps\Fubar.exe
WORKDIR C:\Myapps\Data
EXECUTE
DELETE C:\Myapps\Data\*.*
```

The following script file copies all the .wri files from the directory C:\Write\Files, executes Write.exe in directory C:\Temp.wri, and then removes all files from that directory when the program terminates:

```
PATH C:\Wtsrv\System32\Write.exe
WORKDIR C:\Temp.wri
COPY C:\Write\Files\*.wri C:\Temp.wri
EXECUTE
DELETEALL C:\Temp.wri\*.*
```

The following example demonstrates using the script file to implement a front-end registration utility before executing the application Coolapp.exe. This method can be used to run several applications in succession:

```
PATH C:\Regutil\Reg.exe
WORKDIR C:\Regutil
EXECUTE
PATH C:\Coolstuff\Coolapp.exe
WORKDIR C:\Temp
EXECUTE
DELETEALL C:\Temp
```

AUDITLOG (Generate Logon/Logoff Reports)

Description

The **auditlog** utility generates reports of logon/logoff activity for a MetaFrame server based on the Windows NT Server security Event Log. To use **auditlog**, logon/logoff accounting must be enabled. Report output can be redirected to a file.

Syntax

auditlog [*username* | *session*] [/**eventlog**:*filename*] [/**before**:*mm/dd/yy*] [/**after**:*mm/dd/yy*] [[/**write**:*filename*] | [/**detail** | /**time**] [/**all**]]

auditlog [*username* | *session*] [/**eventlog**:*filename*] [/**before**:*mm/dd/yy*] [/**after**:*mm/dd/yy*] [[/**write**:*filename*] | [/**detail**] | [/**fail** | /**all**]]

auditlog [/**clear**:*filename*]

auditlog [/**?**]

Parameters

username
Specifies a *username* for which to produce a logon/logoff report. Use this to examine the logon/logoff record for a particular user.

session
Specifies the name of a *session* for which to generate a logon/logoff report. Use this to examine the logon/logoff record for a particular session.

Options

/**eventlog**:*filename*
Specifies the name of a backup security Event Log to use as input to **auditlog**. You can create a backup security log from the Event Log Viewer or by using **auditlog** /**clear**:*filename*.

/**before**:*mm/dd/yy*
Reports on logon/logoff activity only before *mm/dd/yy*.

/**after**:*mm/dd/yy*
Reports on logon/logoff activity only after *mm/dd/yy*.

/**write**:*filename*
Specifies the name of an output file. Creates a comma-delimited file that can be imported into an application such as a spreadsheet to produce custom reports or statistics. It generates a report of logon/logoff activity for each user, displaying logon/logoff times and total time logged on.

If *filename* exists, the data is appended to the file.

/**time**
Generates a report of logon/logoff activity for each user, displaying logon/logoff times and total time logged on. Useful for gathering usage statistics by user.

/**fail**
Generates a report of all failed logon attempts.

/**all**
Generates a report of all logon/logoff activity.

/**detail**
Generates a detailed report of logon/logoff activity.

/**clear**:*filename*
Saves the current event log in *filename* and clears the Event Log. This command will not work if *filename* already exists.

/**?** (help)
Displays the syntax for the utility and information about the utility's options.

Remarks

Auditlog gives you a powerful tool to verify and maintain system security and correct usage. The information can be extracted as reports or as comma-delimited files that can be used as input to other programs.

You must enable logon/logoff accounting on the local machine in order to collect the information used by **auditlog**. To enable logon/logoff accounting, logon as a local administrator and start User Manager for Domains. On the **User** menu, click **Select Domain**. Enter the name of the local machine and click **OK**. On the **Policies** menu, click **Audit** and check the **Logon Success** and **Failure** boxes. Click **OK** to save your changes.

CHANGE CLIENT (Change ICA Client Device Mapping Settings)

Description

Change client changes the current ICA Client device mapping settings.

Syntax

change client [/**view** | /**flush** | /**current**]

change client **[**{/**default** | [/**default_drives**] | [/**default_printers**]} [/**ascending**]] [/**noremap**] [/**persistent**] [/**force_prt_todef**] [/**delete** *host_device*] [*host_device client_device*] [/**?**]

Parameters

host_device
Specifies the name to be given to a mapped client device.

client_device
Specifies the name of a device on the client to be mapped to *host_device*.

Options

/**view**
Displays a list of all available client devices. Type **net use** to display current client device mappings.

/**flush**
Flushes the client drive mapping cache. This forces the MetaFrame server and the client to resynchronize all disk data.

/**current**
Displays the current ICA Client device mappings.

/**default**
Resets host drive and printer mappings to defaults.

/**default_printers**
Resets host printer mappings to defaults.

/**default_drivers**
Resets host drive mappings to defaults.

/**ascending**
Uses ascending, instead of descending, search order for available drives and printers to map. This option can only be used with /**default**, /**default_drives**, or /**default_printer**.

/**noremap**
If /**noremap** is specified, client drives that conflict with MetaFrame drives are not mapped.

/**persistent**
Saves the current client drive mappings in the user's profile.

/**force_prt_todef**
Sets the default printer for the MetaFrame client session to the default printer on the client's Windows desktop.

/**delete** *host_device*
Deletes the client device mapping to *host_device*.

/**?** (help)
Displays the syntax for the utility and information about the utility's options.

Remarks

Typing **change client** with no parameters displays the current ICA Client device mappings. This is equivalent to typing **change client /current**.

Use **change client** *host_device client_device* to create a client drive mapping. This maps the *client_device* drive letter to the letter specified by *host_device*; for example, **change client v: c:** maps client drive C to drive V on the MetaFrame server.

The /**view** option displays the share name, the share type, and a comment describing the mapped device. Sample output for **change client /view** follows:

```
C:\Wtsrv\Profiles\adamm>change client /view
Available Shares on client connection ICA-tcp#7

SHARENAME       TYPE            COMMENT
--------------- --------------- -------------
\\Client\A:     Disk            Floppy
\\Client\C:     Disk            FixedDrive
\\Client\D:     Disk            CdRom
\\Client\LPT1:  Printer         Parallel Printer
\\Client\COM1:  Printer         Serial Printer
```

The **/flush** option flushes the client drive cache. This cache is used to speed up access to client disk drives by retaining a local copy of the data on the MetaFrame server. The timeout for hard drive cache entries is ten minutes and the timeout for diskette data is five seconds. If the client PC is using a multitasking operating system and files are created or modified, the MetaFrame server does not know about the changes. Flushing the cache forces the data on the MetaFrame server to be synchronized with the client data. The cache timeout for diskettes is set to five seconds because diskette data is usually more volatile; that is, the diskette can be removed and another diskette inserted.

The **/default** option maps the drives and printers on the client PC to mapped drives and printers on the MetaFrame server. The A and B drives are always mapped to A and B on the MetaFrame server. Hard drives are mapped to their corresponding drive letters if those drive letters are available on the MetaFrame server. If the corresponding drive letter is in use on the MetaFrame server, the default action is to map the drive to the highest unused drive letter. For example, if both machines have C and D drives, the client C and D drives are mapped to V and U respectively. These default mappings can be modified by the /**ascending** and /**noremap** options.

The **/default_printers** option resets host printer mappings to defaults. /**default_printers** attempts a one-to-one mapping of all client printers; for example, client LPT1 and LPT2 are mapped to server LPT1 and LPT2. If the /**ascending** option is specified, the mapping is done in ascending order.

The **/default_drives** option resets host drive mappings to defaults. /**default_drives** attempts a one-to-one mapping of all client drives; for example, client A and B drives are mapped to user drives A and B. Client hard drives are mapped unless there is a MetaFrame drive with the same letter, in which case the client drive is mapped to the next available drive letter going backwards from V. If the /**ascending** option is specified, the mapping is done in ascending order.

The /**ascending** option causes the mapping to occur in ascending drive letter order. For example, if the first two available drive letters on the MetaFrame server are I and J, the C and D drives in the preceding example are mapped to I and J respectively.

The /**noremap** option causes the mapping to skip drive letters occupied on the MetaFrame server. For example, if the MetaFrame server has a C drive but no D drive, the client's D drive is mapped, but not the C drive.

The **/persistent** option causes the current device mappings to be saved in the user's profile. Note that drive conflicts can occur if the user logs on from another client PC with different disk drives or logs onto a MetaFrame server with a different disk drive configuration.

The **/force_prt_todef** option sets the default printer for the Citrix ICA Client session to the default printer on the client's Windows desktop.

Security Restrictions

None.

CLTPRINT (Set the Number of Client Printer Pipes)

Description

Sets the number of printer pipes to the client print spooler.

Syntax

cltprint [/**q**] [/**pipes**:*nn*] [/**?**]

Options

/**q**
Displays the current number of printer pipes.

/**pipes:***nn*
Sets the specified number of printer pipes. This number must be between 10 and 63.

/**?** (help)
Displays the syntax for the utility and information about the utility's options.

Remarks

Printer pipes are used to send data from applications to client print spoolers. The number of pipes specifies the number of print jobs that can be sent to the spooler simultaneously.

The default number of printer pipes is ten.

The **Spooler** service must be stopped and restarted after changing the number of pipes. Print jobs already spooled continue printing.

Print jobs sent to the spooler will get an error message. Make sure no users start printing during the time the spooler service is stopped.

ICAPORT (Configure TCP/IP Port Number)

Description

Configures the TCP/IP port number used by the ICA protocol on the MetaFrame server.

Syntax

icaport {/**query** | /**port**:*nnn* | /**reset**} [/**?**]

Options

/**query**
Queries the current setting.

/**port**:*nnn*
Changes the TCP/IP port number.

/**reset**
Resets the TCP/IP port number to 1494, which is the default.

/**?** (help)
Displays the syntax for the utility and information about the utility's options.

Remarks

Use **icaport** to change the TCP/IP port number used by the ICA protocol. The default port number is 1494. The port number should be in the range of 0–65535 and must not conflict with other well-known port numbers. Whenever the port number is changed, the server must be restarted for the new value to take effect. If you change the port number on the MetaFrame server, you must also change it on every Citrix ICA Client that will connect to that server. For instructions on changing the port number on Citrix ICA Clients, see the *Citrix ICA Client Administrator's Guides* for the ICA Clients that you plan to deploy.

Example

To set the TCP/IP port number to 5000:

```
icaport /port:5000
```

To reset the port number to 1494:

```
icaport /reset
```

Security Restrictions

Only administrators can run **icaport**.

NDSPSVR (Enable or Disable a Preferred Server for NDS Logons)

Description

Use **ndspsvr** to enable or disable a preferred server for NDS logons.

Syntax

ndspsvr {/**query** | /**enable**:*fileservername* | /**disable**} [/**?**]

Options

/**query**
Queries the current setting.

/**enable**:*fileservername*
Enables the preferred server.

/**disable**
Disables the preferred server.

/**?** (help)
Displays the syntax for the utility and information about the utility's options.

Remarks

By default, MetaFrame uses the first NetWare directory server listed in the bindery of the preferred NetWare server (or the first NetWare server to respond to a Query Nearest Server broadcast) for NDS logons. When the server is located across a WAN link this can cause delays in logon processing. Use the **ndspsvr** command to specify a local NDS directory server.

Any changes made take effect the next time the MetaFrame server is rebooted.

Security Restrictions

Only administrators can use **ndspsvr**.

QUERY ACL (Security Audit Utility)

Description

This command is identical to **aclcheck**. It performs a file security audit on the specified directory or drive letter. **Query acl** reports file accesses allowed by accounts other than Administrator, Administrators, or SYSTEM. **Query acl** can also generate a report of registry keys that have Delete, Write, Add, Link, Change Permissions, or Take Ownership permissions for non-administrator users. The system security level (Low, Medium, or High) is also reported.

Syntax

query acl [*path*] [/**registry_only** | /**files_only** [/**ignore_execute**]] [/**?**]

Parameter

path
The name of the drive or directory path to audit.

Options

/**ignore_execute**
Does not report files with user Execute permissions.

/**registry_only**
Checks only the system registry.

/**files_only**
Checks only disk files.

/**?** (help)
Displays the syntax for the utility and information about the utility's options.

Remarks

Query acl generates a report of potential security exposures on a MetaFrame server. **Query acl** reports excessive file or registry accesses allowed by accounts other than Administrator, Administrators, and SYSTEM.

The file report shows any files that have Delete, Write, Append, Execute (unless the /**ignore_execute** option is specified), Change Permissions, or Take Ownership permissions for non-administrator users.

The registry report shows any registry keys that have Delete, Write, Add, Link, Change Permissions, or Take Ownership permissions for non-administrator users.

If no arguments are specified, **query acl** checks all local drives and then checks the **HKEY_LOCAL_MACHINE** portion of the system registry.

Any files or registry keys that non-administrator users can write to are reported in the following format:

```
OBJECT  INHERIT ACCOUNT       FILE
_______ _______ ____________ ____________________________________
DWXPO           \Everyone     C:\Autoexec.bat
X               \Everyone     C:\boot.ini
DWXPO           \Everyone     C:\Config.sys
X       X       \Everyone     C:\Wtsrv
```

Query acl also audits the MetaFrame execute list (created and maintained by the Application Security utility) to verify that no executable files in the execute list are writable by users.

QUERY LICENSE (View Citrix Licenses)

Description

Query license displays information about Citrix licenses.

Syntax

query license [/**server**:*servername* | /**all**] [/**?**]

Options

/**server**:*servername*
The Citrix server to be queried. The default is the current Citrix server.

/**all**
Displays information about all licenses on the network.

/**?** (help)
Displays the syntax for the utility and information about the utility's options.

Remarks

Query license displays information about the Citrix licenses currently installed on the server.

Security Restrictions

None.

QUERY SERVER (View Citrix Servers)

Description

Query server displays information about the available Citrix servers on the network.

Syntax

query server [*servername*] [/**ping]** [/**count:***n*] [/**size:***n*]

query server [*servername*] [/**stats** | /**reset** | /**load** | /**addr**]

query server [/**tcp**] [/**ipx**] [/**netbios**] [/**tcpserver**:*x*]
[/**ipxserver**:*x*] [/**netbiosserver**:*x*]
[/**license** | /**app** | /**gateway** | /**serial** | /**disc** | /**serverfarm** | /**video**]
[/**continue**] [/**?**]

Parameter

servername
The name of a Citrix server.

Options

/**tcp**
Displays TCP/IP information.

/**ipx**
Displays IPX information.

/**netbios**
Displays NetBIOS information.

/**tcpserver**:*x*
Sets the TCP/IP default server address to *x*.

/**ipxserver**:*x*
Sets the IPX default server address to *x*.

/**netbiosserver**:*x*
Sets the NetBIOS default server address to *x*.

/**license**
Displays user licenses.

/**app**
Displays application names and server load.

/**gateway**
Displays configured gateway addresses.

/**serial**
Displays license serial numbers.

/**disc**
Displays disconnected session data.

/**serverfarm**
Displays server farm names and server load.

/**video**
Displays VideoFrame servers.

/**ping**
Pings selected server.

/**count**:*n*
Number of times to ping (default: 5).

/**size**:*n*
Size of ping buffers (default: 256 bytes).

/**stats**
Displays browser statistics on the selected server.

/**reset**
Resets browser statistics on the selected server.

/**load**
Displays load data on selected server.

/**addr**
Displays address data on selected server.

/**continue**
Don't pause after each page of output.

/**?** (help)
Displays the syntax for the utility and information about the utility's options.

Remarks

Query server uses the ICA Browser to display data about the Citrix servers present on a network.

Query server with no parameters is the same as **query server /tcp /ipx /netbios**.

On a server with two network cards, the **query server** command only enumerates servers on one card's subnet at a time. To enumerate the servers on the other card's subnet, specify the address of any server on the subnet with the **/tcpserver**:*x*, **/ipxserver**:*x*, or **/netbiosserver**:*x* parameter.

Security Restrictions

None.

APPENDIX B

Citrix DirectICA for MetaFrame

Overview

Citrix DirectICA for MetaFrame adds support for multi-VGA adapters to Citrix MetaFrame Application Server for Windows. A *multi-VGA adapter* (also called a *multiconsole adapter*) is a hardware device that contains several VGA video adapters with additional support hardware. Each multi-VGA adapter appears to the server as several VGA video adapters, each with an accompanying keyboard, mouse, and optional serial and parallel ports, depending on the manufacturer and model. The only limit to the number of multi-VGA adapters that you can install is your license count.

The combination of a keyboard, mouse, and monitor attached to a port on the multi-VGA adapter is referred to as a *DirectICA station.* MetaFrame treats connections associated with DirectICA stations much like the system console; the devices (serial and parallel ports) associated with the DirectICA station are on the server computer itself. Any serial or parallel ports associated with a DirectICA station are given unique device names and are treated as ports on the server computer. Because the ports are on the server, DirectICA stations do not support drive mapping, COM port mapping, or printer mapping.

System Requirements

See the "System Sizing" section in Chapter 1 for general MetaFrame hardware requirements.

DirectICA has been tested with the following multi-VGA products:

- Maxspeed SGX MaxStation and PCI MaxStation adapters and optional Maxspeed MaxRack bus expansion system and appropriate cabling and MaxStation base units
- Stone Microsystems MultiVideo VGA System ISA adapter with 512K or 1MB modules and appropriate cabling and junction boxes
- Stone Microsystems CenterNET 2 PCI adapter with appropriate cabling and station boxes

Restrictions

The server console cannot support more than 256 colors when DirectICA is installed.

Some video adapters are not compatible with DirectICA in all modes; in those cases you must use the standard VGA video driver, which limits the console to 640 x 480 resolution.

The following restrictions apply to DirectICA stations:

- Shadowing is not supported.
- Encryption is not supported.
- Published applications and load balancing are not supported.
- DirectICA stations are reset as soon as a user logs out or disconnects. Users cannot reconnect to disconnected sessions.

Installation

Before installing DirectICA, read "System Requirements" earlier in this appendix to ensure your MetaFrame server meets the minimum requirements for DirectICA.

Note Some video adapters are not compatible with DirectICA in all modes. In those cases you must use the standard VGA video driver, which limits the server console to 640 x 480 resolution.

Hardware Installation

This section contains separate installation procedures for the Maxspeed and Stone Microsystems adapters.

You can install as many multi-VGA adapters as your system can contain, but they must all be from the same manufacturer.

▶ To install the Maxspeed MaxStation adapter

Before installing, decide which base address to use with your multi-VGA adapter. The base address chosen must not conflict with other devices in your server. If you do not have a record of which address ranges are already being used, check your BIOS configuration software and system and expansion card documentation. Although the base address for the Maxspeed card is software configurable, check the jumper settings on existing expansion cards when you open the server to install the multi-VGA adapter.

- Install the multi-VGA adapter(s) and connect the DirectICA stations according to the manufacturer's documentation.

Note The serial port on each DirectICA station is reserved for use with a mouse.

▶ To install the Stone Microsystems adapter

The Stone Microsystems adapter uses interrupt requests (IRQs) for the DirectICA station keyboards and serial devices. Before installing, decide which IRQs and base address to use with your multi-VGA adapter. The IRQs and base address chosen must not conflict with other devices in the server.

If you do not have a record of which IRQs and address ranges are already being used, check your BIOS configuration software and system and expansion card documentation. Check the jumper settings on existing expansion cards when you open the server to install the multi-VGA adapter.

1. Configure the base address using the jumper settings on the adapter. See the manufacturer's documentation for instructions. Make a note of the address you use.
2. Install the multi-VGA adapter(s) and connect the DirectICA stations according to the manufacturer's documentation.

Note The first serial port on each DirectICA station is reserved for use with a mouse only.

Software Installation

▶ **To install DirectICA**

1. Log on to the MetaFrame server as an administrator.
2. Insert the MetaFrame CD-ROM.
3. Click the **Start** button and then click **Run**. Type ***d*:\drctica\setup.exe** where *d:* is the letter of the CD-ROM drive.
4. The installation wizard guides you through the setup process.
5. A dialog appears asking you to read the Readme file. This file contains information not available at the time of printing this manual as well as useful information regarding the hardware setup.
6. If you have an ISA multi-VGA card, a dialog appears asking if you want to run DirectICA Configuration to manually set the IRQs or base address.

   By default, the DirectICA driver automatically selects an available base address (for the Maxspeed adapter) or IRQs (for the Stone Microsystems adapter) each time the driver is loaded during bootup. In most cases, you do not need to change these defaults. If desired, you can manually assign the IRQs or base address.

   Warning If the IRQ or base address settings conflict with other devices on the system, incorrect system operation (including rendering the system unbootable) can occur.

7. Restart the MetaFrame server. Watch the startup sequence to make sure the DirectICA driver loads successfully and detects the DirectICA stations. If you experience problems, see "Troubleshooting" later in this appendix.
8. After the MetaFrame server restarts, see "Enabling DirectICA Stations" later in this appendix for instructions on enabling the DirectICA stations.

Uninstalling DirectICA

If DirectICA is uninstalled, the Microsoft client licenses used by DirectICA stations are unavailable for other clients to use. If you reinstall DirectICA, the DirectICA stations are automatically re-created with the same names so that the Microsoft client licenses are reused with the DirectICA stations.

▶ **To uninstall DirectICA**

1. Make sure all users are logged off from DirectICA stations.
2. Log on using the local "Administrator" account.
3. Click the **Start** button, point to **Settings**, and then click **Control Panel**.
4. Double-click **Add/Remove Programs** to display the **Add/Remove Programs** dialog box.
5. Select **Citrix DirectICA for MetaFrame** and click **Add/Remove**.
6. Click **Yes** when the confirmation dialog box appears.
7. The DirectICA uninstall process begins. When it completes, click **OK**.
8. Click **OK** when the dialog box suggesting you reboot the server appears. This does not reboot the server.
9. Click **OK** to close the **Add/Remove Programs** dialog box.
10. Reboot the MetaFrame server.

Configuring DirectICA

Citrix DirectICA provides two programs used for configuring DirectICA stations: DirectICA Configuration and Citrix Connection Configuration. These programs are located in the **MetaFrame Tools** program folder.

Use DirectICA Configuration to:

- Set the base address or IRQ settings for a multi-VGA adapter
- Display version information about Citrix DirectICA (if the multi-VGA adapter driver fails to load, the **About** tab displays an error message)

Citrix Connection Configuration looks and works like Terminal Connection Configuration, but has additional support for DirectICA. DirectICA connections can be added, copied, and deleted just like connections for other transports.

Enabling DirectICA Stations

Before using DirectICA stations, DirectICA connections must be added using Citrix Connection Configuration. You must restart the server after installing DirectICA before you can perform this procedure.

▶ **To add DirectICA connections**

1. Logon to the MetaFrame server as an administrator.
2. Click the **Start** button, point to **Programs**, point to **MetaFrame Tools**, and then click **Citrix Connection Configuration**.

3. On the **Connection** menu, click **New**. The **New Connection** dialog box appears.
4. Enter a name for this connection in the **Name** box.
5. In the **Type** list, click **Citrix DirectICA**.
6. If desired, enter a comment in the **Comment** box.
7. Select the DirectICA station for which to create the session. Only the stations that do not yet have connections configured are listed.
8. If desired, click **Video Settings** to change the color palette, resolution, font size, and refresh frequency for the DirectICA station. See "Changing the Video Settings for DirectICA Stations" later in this appendix for more information.
9. Click **OK** to close the **New Connection** dialog box.

   The DirectICA station is activated and the Windows Logon screen is displayed.

Note You must have sufficient Microsoft licenses for each activated DirectICA station. If there are not sufficient licenses, the station is not activated and an error is logged to the application error log. Use Event Viewer to view the application log.

Changing the Video Settings for DirectICA Stations

Users do not have permission to change their video settings (color palette, resolution, font size, and refresh frequency). Administrators can change these settings using the **Video Settings** button on the **Edit Connection** dialog box in Citrix Connection Configuration.

Serial Port Support on DirectICA Stations

The first serial port on a DirectICA station is a dedicated mouse port, but the second serial port is a system-wide device with the designation **dcom*x***, where *x* is the DirectICA station number. This port can be used with a serial printer, modem, or any general serial communications device.

Serial port support is manufacturer-dependent and not a function of the DirectICA software. At present, only Maxspeed MaxStations support using these ports with DirectICA for MetaFrame.

The serial port specifications are as follows:

- Maximum baud rate: 38400
- Handshaking: XON/XOFF or RTS/CTS

- The DTR (Data Terminal Ready) and DSR (Data Set Ready) modem signals are not supported
- The RI (Ring Indicator) modem signal is not supported; most applications use CD (Carrier Detect) instead

Some applications can only access COM1 or COM2. In this case, you can reassign this port using the **change port** command; for example **change port com1: = dcom*x***, where *x* is the DirectICA station number for which to reassign the port.

Note Serial port operation does not depend on the status of the DirectICA station. The serial port is available even if the DirectICA station is disabled.

Printing to DirectICA Ports

The printer port and second COM port on Maxspeed MaxStations are system-wide devices. All users logged on to that MetaFrame server can print to printers connected to these ports. These printers can also be shared across a network. Just like printer ports physically connected to a Windows NT server, only administrators can add printers connected to Maxspeed MaxStation printer ports.

Serial and printer port support is manufacturer-dependent and not a function of the DirectICA software. At present, only Maxspeed MaxStations support using these ports with DirectICA for MetaFrame.

Note Printer port operation does not depend on the status of the DirectICA station. The printer port is available even if the DirectICA station is disabled.

▶ **To add a printer connected to a DirectICA station**

1. Open the **Printers** folder: click the **Start** button, point to **Settings**, and then click **Printers**.
2. Double-click **Add Printer**.
3. Select **My Computer** and click **Next**.
4. In the **Available ports** box, select the port the printer is connected to and then click **Next**.

   The DirectICA parallel ports are listed as \\.\DLPT*x* and the DirectICA COM ports are listed as \\.\DCOM*x*, where *x* is the station number of the DirectICA station.
5. Continue following the instructions of the **Add Printer Wizard.**

Troubleshooting

This section contains information to help you diagnose and solve common problems encountered with DirectICA.

Note Contact your hardware manufacturer for help with hardware problems.

General Guidelines

Check the messages that appear during the "blue screen" phase of system startup for error messages relating to the multi-VGA adapter.

Check the Event Viewer for error messages.

If your server fails to restart properly after installing DirectICA, restart your system using the "last known good" option. This removes the DirectICA registry settings added during installation and effectively uninstalls the multi-VGA adapter. You should then investigate device conflicts.

If the server's keyboard or mouse does not function properly, try disconnecting the mouse from the server and rebooting. This can help if there is an IRQ conflict. You should then investigate device conflicts.

If the system still does not boot, try removing the multi-VGA adapter.

Installation Problems

If DirectICA does not report the correct number of channels on your multi-VGA adapter after installation, try shutting down the server and then physically turning the power off and then back on (wait at least a minute before turning back on). Some older motherboards do not fully reset the adapter when a software reset is performed.

BIOS Setup

Make sure the BIOS on your system is not using the RAM address space occupied by the base address of the multi-VGA adapter. Some motherboards may use this address space to shadow system or video BIOS. If this is the case, disable the shadowing feature.

You may need to use a third-party program (such as Intel's ISA Configuration Utility [ICU]) to restrict PCI adapters from using the IRQs and base address of the multi-VGA adapter.

Base Address Conflicts with Maxspeed Adapters

If the DirectICA stations display a logon screen but the mice and keyboards do not work, a base address conflict is the likely cause. Compare the base address used by the multi-VGA adapter with the address ranges used by other devices on the server to see if there is a conflict.

To change the base address of a Maxspeed MaxStation adapter, run DirectICA Configuration, change the base address to the appropriate value, and then restart the system.

IRQ Conflicts with Stone Microsystems Adapters

IRQ conflicts can cause the following symptoms:

- DirectICA station keyboards do not work but the main console keyboard works
- Mice do not work

To solve these conflicts, run DirectICA Configuration, disable autoselection of IRQs, and then select IRQs manually. The new settings take effect when you restart the system.

DirectICA Stations do not Display the Windows Logon Screen

If a DirectICA station does not display the Windows Logon screen after you have added a connection using Citrix Connection Configuration, verify that you have sufficient Microsoft licenses for all active DirectICA stations and that there are no licensing errors in the application error log. Use Event Viewer to view the application error log.

APPENDIX C

ICA Browser Registry Keys

You do not normally need to override the default values for ICA Browser registry entries. However, for some systems you can adjust individual parameters to suit your particular needs.

▶ **To edit the registry**

1. Click the **Start** button and then click **Run**.
2. Type **regedt32** and click **OK** to load the Registry Editor.

For detailed information on how to add a parameter to a key in the registry, see the online Help for the Registry Editor.

Warning Make a backup of your registry before changing any settings. See the Terminal Server documentation for instructions on making a backup of the registry.

ICA Browser Registry Key Values

The ICA Browser variables are in the following registry path:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ICABrowser\Parameters

Important If any of the registry variables below are changed, the ICA Browser must be stopped and restarted for the new values to take effect. The ICA Browser can be stopped and started using the **Services** icon in Control Panel. When the browser is restarted, a new election takes place using the changed values.

AckRetries REG_DWORD **0 - 0xffffffff** **(3 = default)**

Specifies the number of times the browser tries to send a master browser update before forcing a browser election.

AckTimeout REG_DWORD **0 - 0xffffffff seconds (5 = default)**
Specifies the interval a browser waits for an ACK after sending a master browser update. If no ACK is received, the browser resends the update. The browser retries **AckRetries** times before forcing a browser election.

AgeDatabaseTime REG_DWORD **0 - 0xffffffff seconds (300 = default)**
Indicates how frequently the master browser checks the "time to live" value associated with browser data. If the browser data is not being updated, the data is deleted. This value can be set to zero to disable aging of browser data.

ClientElectionTime REG_DWORD **0 to 0xffffffff seconds (30 = default)**
After receiving an election request (BR_ELECTION) from a client, all subsequent client initiated election requests are ignored for **ClientElectionTime** seconds. This allows the original election to complete before another election is allowed.

DisableEnumeration REG_DWORD **0 or 1 (0 = default)**
Setting this value to 1 prevents the computer name of this Citrix server from appearing in the clients' server list. All configured published application names still appear in the clients' server list. This provides a way to *hide* a server.

DisableGateway REG_DWORD **0 - 1 (0 = default)**
Setting this value to 1 causes this browser to ignore all configured gateway addresses. It also prevents this browser from accepting gateway data from another browser.

DisableIpx REG_DWORD **0 - 1 (0 = default)**
Setting this value to 1 prevents this browser from participating on IPX networks.

DisableNetBios REG_DWORD **0 - 1 (0 = default)**
Setting this value to 1 prevents this browser from participating on NetBIOS networks.

DisableTcp REG_DWORD **0 - 1 (0 = default)**
Setting this value to 1 prevents this browser from participating on TCP/IP networks.

GatewayAddTime REG_DWORD **0 to 0xffffffff seconds (1800 = default)**
Indicates how frequently the browser sends the gateway add command (BR_GATEWAY_ADD). The gateway add command configures all gateways that are specified in the registry by **GatewayIpx** and **GatewayTcp**.

GatewayIpx REG_MULTI_SZ **Citrix server addresses**

To set up an IPX gateway the remote IPX address (network:node) of a Citrix server must be specified in this list.

When a master browser receives an update from a browser, it forwards the data to all configured gateways on the same network protocol.

It does not matter which Citrix server the gateway address is configured on. The same address can be configured on multiple Citrix servers.

GatewayTcp REG_MULTI_SZ **Citrix server addresses**

To set up a TCP/IP gateway, the remote IP address (or DNS name) of a Citrix server must be specified in this list.

When a master browser receives an update from a browser, it forwards the data to all configured gateways on the same network protocol.

It does not matter which Citrix server the gateway address is configured on. The same address can be configured on multiple Citrix servers.

IsMasterBrowser REG_DWORD **0 - 1** **(0 = default)**

When this value is set to 1, it raises the browser's priority during a master browser election. As long as no other system has this value set, this system becomes the master browser.

LoadLevelBoost REG_DWORD **0 to 0xffffffff** **(10 = default)**

After a server is selected on a load balance request, **LoadLevelBoost** is added to the load level of the server. When two servers have nearly identical loads, this prevents the same server from being selected on the next request. This boost is overwritten on the next browser data update.

LogFlush REG_DWORD **0 or 1** **(0 = default)**

When this value is set to 1, all log events are immediately written to disk as they occur, without any buffering. This has a significant performance penalty and should only be used for problem determination.

LogMask REG_DWORD **0 - 0xffffffff (0 = default)**
Specifies a bit mask for logging debug information. After changing this value, stop and start the ICA Browser to start logging to the file %systemRoot%\Ibrowser.log. The bit mask values are:

Bit Mask	Description
0x00000001	browser initialization
0x00000002	browser elections
0x00000004	browser updates
0x00000008	gateway updates
0x00000010	client requests
0x00000020	reads and writes
0x00000040	reads and writes data
0x00000080	database updates
0x00000100	browser data
0x00000200	load balancing
0x10000000	timers
0x20000000	semaphores

LogToDebugger REG_DWORD **0 - 1 (0 = default)**
Specifies that logging messages should be written to the kernel debugger in addition to the log file.

MasterDeclareTime REG_DWORD **0 - 0xffffffff seconds (3600 = default)**
Indicates how frequently the master browser broadcasts a master declare. A *master declare* is used to detect multiple master browsers on the same network. If a master browser ever receives this packet from another browser, it forces an election to get rid of the extra master browser. This value can be set to zero to disable master browser declares.

NotMasterBrowser REG_DWORD **0 or 1 (0 = default)**
When this value is set to 1, it lowers the browser's priority during a master browser election. This prevents this browser from becoming the master browser.

PingAddressTime REG_DWORD **0 to 0xffffffff seconds (5 = default)**
Specifies the time a browser waits, after sending a ping request, for a ping reply. If no ping reply is received, the browser tries to send the update again. The browser uses pings to verify a server still exists before returning the address of a server to the client.

RefreshDelay REG_DWORD **0 - 0xffffffff seconds (30 = default)**
Specifies the delay after a client connects or disconnects from the Citrix server before a master browser update is sent. This delay should be large enough to let the system "settle" before sending the master browser update.

SendRetries REG_DWORD **0 - 0xffffffff (3 = default)**
Specifies the number of times the browser sends a gateway add or delete command.

UpdateTime REG_DWORD **0 - 0xffffffff seconds (1800 = default)**
Indicates the frequency with which the browser updates the master browser. After an election all browsers know the address of the master browser. After a random delay (4-6 seconds) each browser sends an update datagram to the master browser. After this initial update, the browsers update the master browser every **UpdateTime** seconds. Upon receiving data from a browser, the master browser replies with an ACK. Master browser updates are also sent whenever a client connects or disconnects from the Citrix server. Lowering this time makes browser data more accurate, but increases the CPU and network load. Lower this value when load balancing is used. This value can be set to zero to disable periodic updates.

Version REG_DWORD **0 to 0xffffffff**
Specifies the current browser version.

Load Balancing Registry Key Values

The following registry entries are configured using the **Adjust Load Balancing** dialog box in the Load Balancing Administration program. It is suggested that you only use that program for modifying these values. They are listed here for completeness.

AppName REG_MULTI_SZ **One or more text strings**
Specifies a list of one or more application names used for load balancing. The application name can be thought of as a server farm name. To configure load balancing, two or more systems must be configured with the same application name. The application name can appear in the client's server list along with the other Citrix servers. When the client selects an application name, the master browser returns the Citrix server address with the least load, based on the following factors.

Weighting Factor	Limit	Description
BalanceICA Connections	Configured ICA connections	Number of free ICA connections
BalanceUserLicenses	BalanceMaxUserLicenses	Number of free user licenses
BalancePageFile	BalanceMinPageFile	Size of remaining page file
BalancePageFaults	BalanceMaxPageFaults	Number of page faults
BalanceMemoryLoad		Memory load level
BalanceProcessorBusy		Processor load

BalanceBias REG_DWORD **0 - 0xffffffff (0 = default)**
After all load balance calculations are done, **BalanceBias** is added to the resulting load level. An idle system has a very small load level, a busy system a larger load level. By specifying a positive number here, a system can be made to look busier than it actually is. By specifying a negative number (for example, 0xfffffff0) a system can be made to look less busy.

BalanceMaxPageFaults REG_DWORD **0 - 0xffffffff (1000 = default)**
Specifies the maximum number of page faults used for load balance calculations.

BalanceMaxUserLicenses REG_DWORD **0 - 0xffffffff (10 = default)**
By changing this value, the maximum number of user licenses used for load balance calculations can be limited. Load balance calculations use the lesser of **BalanceMaxUserLicenses** and the number of installed user licenses. Load balancing will never select a system that does not have at least one available user license.

BalanceMemoryLoad REG_DWORD **0 - 1000 (100 = default)**
Specifies the memory load weighting factor. Each of the weighting factors is divided by the sum of the weighting factors to arrive at ratios that are used to compute the system load level. The memory load is calculated by the following algorithm:

```
if  (available memory pages < 100) then
    memory load = 100 * memory load ratio
else
    memory load = (100 - ((available memory pages - 100) / 10))* memory
    load ratio
```

Increasing **BalanceMemoryLoad** gives more "weight" to memory load in computing the load level. Setting this value to 0 causes load balancing to ignore memory load.

BalanceMinPageFile REG_DWORD **0 - 0xffffffff (500 = default)**
Specifies the minimum number of free bytes that must be present in the page file for load balancing to select the system.

BalancePageFaults REG_DWORD **0 - 1000** **(100 = default)**
Specifies the page fault weighting factor. Each of the weighting factors is divided by the sum of the weighting factors to arrive at ratios that are used to compute the system load level. The page fault load is calculated by dividing number of page faults by **BalanceMaxPageFaults** and multiplying by the page file ratio. Making **BalancePageFaults** higher gives more "weight" to page faults in computing the load level. Setting this value to zero (0) causes load balancing to ignore page faults.

BalancePageFile REG_DWORD **0 - 1000** **(10 = default)**
Specifies the page file weighting factor. Each of the weighting factors is divided by the sum of the weighting factors to arrive at ratios that are used to compute the system load level. The page file load is calculated by dividing the number of free bytes in the page file by the total number of bytes in the page file and multiplying by the page file ratio. Making this number higher gives more "weight" to the page file in computing the load level. Setting this value to zero (0) causes load balancing to ignore the page file. Load balancing never selects a system that does not have at least **BalanceMinPageFile** bytes left in the page file.

BalanceProcessorBusy REG_DWORD **0 - 1000** **(100 = default)**
Specifies the processor weighting factor. Each of the weighting factors is divided by the sum of the weighting factors to arrive at ratios that are used to compute the system load level. The processor load is calculated by multiplying by the processor busy percentage by the processor busy ratio. Increasing this value gives more "weight" to processor load in computing the load level. Setting this value to zero (0) causes load balancing to ignore the processor load.

BalanceUserLicenses REG_DWORD **0 - 1000** **(10 = default)**
Specifies the user license weighting factor. Each of the weighting factors is divided by the sum of the weighting factors to arrive at ratios that are used to compute the system load level. The user license load is calculated by dividing the number of free user licenses by the number of installed user licenses and multiplying by the user license ratio. The maximum number of user licenses used for this calculation can be set by changing **BalanceMaxUserLicenses**. Increasing **BalanceUserLicenses** gives more "weight" to the number of free user licenses in computing the load level. Setting this value to zero (0) causes load balancing to ignore the number of free user licenses. Load balancing never selects a system that does not have at least one available user license.

BalanceICAConnections REG_DWORD **0 - 1000** **(10 = default)**

Specifies the ICA connection weighting factor. Each of the weighting factors is divided by the sum of the weighting factors to arrive at ratios that are used to compute the system load level. The ICA connection load is calculated by dividing the number of free ICA connections by the number of configured ICA connections and multiplying by the ICA connection ratio. Increasing this number gives more "weight" to the number of free ICA connections in computing the load level. Setting this value to zero (0) causes load balancing to ignore the number of free ICA connections. Load balancing never selects a system that does not have at least one available ICA connection.

Index

1

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W